# DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA AGENCIA DE ADUANAS MOVE CARGO S.A. NIVEL 1.

ANA MARÍA BOHÓRQUEZ MUÑOZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C. - COLOMBIA
2018

# DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA AGENCIA DE ADUANAS MOVE CARGO S.A. NIVEL 1.

ANA MARÍA BOHÓRQUEZ MUÑOZ

Trabajo de grado para optar al título de especialista en seguridad informática

Director:
Anívar Chaves Torres
Ingeniero de sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGICAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C. - COLOMBIA
2018

Nota de aceptación:

_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente de jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá 24 de septiembre del 2018

## AGRADECIMIENTOS

Agradezco a mis padres Noralba Muñoz Reina y Alvaro Bohórquez Moreno por cuidarme, enseñarme y brindarme todo el apoyo incondicional en cada aspecto de mi vida, también agradezco a mi hermana Ginna Paola Bohórquez Muñoz por estar a mi lado, ser un ejemplo y el pilar fundamental en mi vida. Agradezco a mis abuelos por enseñarme lo lindo de la vida y que cada pequeño problema que se presente tiene solución y al final solo las experiencias vividas son las que nos definen como personas.

Agradezco a mi pareja de vida Diego Felipe Hernández Sánchez por apoyarme y acompañarme en mi crecimiento profesional, cuidarme y estar conmigo en todos los momentos difíciles, por realizar los sacrificios que implica tener una familia y ser un excelente compañero.

Agradezco a la Universidad Nacional Abierta y a Distancia “UNAD”, a la facultad de Ciencias Básicas, Tecnológicas e Ingeniería y al Programa de Especialización de Seguridad Informática por desarrollar mis conocimientos en este campo y brindarme las habilidades para poder establecer e implementar el Sistemas de Seguridad de la información en la Agencia de Aduanas Move Cargo S.A Nivel 1. También expreso un especial agradecimiento al Sr. Alvaro Rodríguez por abrir las puertas de Move Cargo y permitirme realizar esta actividad.

Por ultimo agradezco al Ingeniero Anivar Chávez Torres por sus valiosos aportes, orientación y respaldo para la realización del presente proyecto de grado.

## CONTENIDO

## LISTA DE FIGURAS

Pág.

## LISTA DE CUADROS

Pág.

## GLOSARIO

**Amenaza:** Son todos los factores tanto internos como externos que pueden afectar en poca o gran medida a un factor en específico.

**Comercio Exterior:** Es el intercambio de bienes existentes entre una o más naciones por medio de la aplicación de reglamentos convenios u acuerdos de negocio internacionales con el propósito de satisfacer las necesidades tanto del mercado interno lo que generar un mayor mercado e ingresos para las naciones.

**Confidencialidad:** Es el procedimiento por el cual se asegura que la información generada por cualquier medio (digital o físico) solamente será conocida, almacenada, o manipulada por personal autorizado.

**Disponibilidad:** Son los procedimientos que garantizan que la información en cualquiera de sus medios de almacenamiento puedan ser consultados por las personas autorizadas en el momento que se requiera.

**Estándares de seguridad:** Son todas aquellas medidas, procedimientos y responsabilidades encaminadas a mantener Sistemas de Seguridad de la Información eficiente y seguro.

**Exportar:** Es el acto de enviar por medio marítimo, aéreo o terrestre mercancía a otro país aplicando tratados internaciones o acuerdos de comercio exterior.

**Integridad:** son los procedimientos que garantizan que la información en cualquiera de los medios almacenados (digital o físico) estén protegidos contra cualquier modificación, alteración o adiciones no autorizadas.

**Importar:** Es el acto de nacionalizar, introducir y comercializar dentro de un país mercancía de otra nación con el fin de suplir una necesidad.

**Mercancía:** Es un bien que es comercializable entre uno o más compradores y vendedores.

**Normas ISO 27001:** Es la norma técnica avalada internacionalmente en la que figuran los requisitos mínimos necesarios para el diseño, implementación y mejora de un Sistema de Gestión de Seguridad de la Información.

**Peligro:** Es la medida calificable sobre los daños que se pueden ocasionar. Estos pueden ser en poca o gran magnitud.

**Riesgo:** Es la probabilidad que un evento se materialice debido a unas características específicas contra el impacto que este genere en un bien específico.

**Seguridad de la información:** Es un conjunto de parámetros, políticas, controles, medios, mecanismo y acciones orientadas a resguardar la información, manteniéndola confidencial, integra y disponible.

**Tratados de libre comercio:** Es un acuerdo comercial entre dos o más naciones para acordar la disminución, concesión de preferencias arancelarias y de reducción de trámites y barreras aduaneras para exportar o importar cualquier tipo de mercancía.

**Vulnerabilidad:** Es la medida en la cual se está expuesto a un peligro, amenaza o riesgos que pudiera causar daños en poca o gran magnitud.

# INTRODUCCIÓN

Tanto para las grandes corporaciones como para las pymes, la información es un activo muy valioso y transcendental para la continuidad de los negocios y su crecimiento en el mercado, pero no toda es valiosa, solo aquella que con el correcto manejo y análisis pueda generar factores de crecimiento, genere una ventaja competitiva o permita dar valor agrado a un producto o servicio. La información que es considerada la más valiosa es aquella relacionada con el consumidor final, el mercado y la competencia, es tan importante que se invierte gran cantidad de esfuerzos, recursos y tiempo formulando, analizado e implementado herramientas metodologías y tecnologías que garanticen que la información siempre se encontrará integra, disponible y confidencial. En algunos casos algunas organizaciones han implementado grandes infraestructuras tecnologías con el fin de resguardar esta información.

Aunque existen muchos mecanismos para protegerla, también existen muchas herramientas y metodologías usadas por delincuentes que de manera ilegal violan los parámetros de seguridad, estos actos se realizan para hurtar, modificar o dañar la información con fines propios o de terceros. Como medida para mantenerla segura, se adecua controles eficaces y acordes con el tamaño y necesidades de cualquier tipo de organización, se utilizan los Sistemas de Gestión Seguridad de la Información (en adelante SGSI), los cuales contiene los mecanismo de seguimiento y control permites para identificar, implementar y realizar seguimiento a la estructura y los recursos con el fin de hallar vulnerabilidades, amenazas y riesgos que pudieran afectar de manera adversa los sistemas de seguridad implementados y por ende la operación de la organización.

La Agencia de Aduanas Move Cargo S.A. Nivel 1. (En adelanta Move Cargo) Consiente del valor de la información generada durante más de 20 años, desea implementar un SGSI dentro de sus instalaciones con el fin de proteger este activo resultado de prestar los servicios de desaduanamiento de mercancías a clientes de alto perfil los cuales exigen especial manejo de sus operaciones y aunque se cuentan con medidas de seguridad implementadas, estas no se encuentran enmarcada en un sistema de gestión por lo cual existen falencias en el control de acceso, manipulación e integridad de la información generado retrasos, reproceso y pérdida de confianza del mercado.

Considerando la necesidad de Move Cargo el presente proyecto tiene el propósito de diseñar un SGSI acorde con su tamaño, necesidades y requisitos, dentro del proyecto se completaron tres objetivos específicos, los cuales tuvieron como meta identificar la situación actual en cuanto a seguridad de la información, diseñar un sistema que permita identificar y evaluar los riesgos y vulnerabilidades que se puedan presentar y por ultimo proponer los controles pertinentes sobre los riesgos considerados como catastróficos y altos.

La estrategia utilizada para diseñar el SGSI consiste en identificar los activos tanto tangibles como intangibles utilizados para administrar y prestar el servicio determinando su nivel de importancia en cuanto al desarrollo normal de sus actividades. Se aplicó una declaración de aplicabilidad a los sistemas informáticos de Move Cargo para determinar su grado de madures identificando factores críticos, riesgosos, vulnerables o que presenten algún tipo de amenaza que pueda generarse tanto interna como externamente ya sea por el medio en el que se desempeña, las actividades que realiza o los sistemas utilizados.

Con la identificación de los activos y los riesgos se realizó una evaluación para determinar el nivel de afectación que se generaría a cada activo en el caso de la materialización de uno de los riesgos, amenazas o vulnerabilidades identificadas y el impacto que este generaría en la prestación del servicio, esta evaluación se realiza analizando la probabilidad de ocurrencia del riesgo contra el impacto que generaría a los activos.

De la evaluación de los riesgos se catalogan aquellos riesgos, vulnerabilidades y amenazas que afectarían a los activos en niveles medios, altos o catastróficos que permitan diseñar controles específicos o políticas de seguridad que permita miniar, eliminar o disminuir los impactos generados por los riesgos.

Como resultado de la ejecución de los tres objetivos se logró desarrollar una declaración de aplicabilidad según norma ISO27001 ajustada a las características de Move Cargo, diseñando un sistema de identificación de vulnerabilidad, evaluación y control de riesgos aplicables en todos los niveles de Move Cargo.

# 1. PROBLEMA

## 1.1 PLANTEAMIENTO DEL PROBLEMA

Para la prestación del servicio de agenciamiento aduanero a nivel nacional para cualquier trámite aduanero (Importaciones, exportaciones, OTM, etc.) es necesario contar con una cantidad de información importante para poder diligenciar los campos de los formularios establecidos por la DIAN, como lo son las 182 casillas de la declaración andina de valor por cada una de las sub partidas que se puedan presentar en un trámite de importación, por temas legales y de control estos procesos debe ser conservada de manera digital y física por un periodo de cinco años a partir de la nacionalización de la mercancía, estas reglamentaciones determinadas por factores externos implican un manejo de información importante que debe ser protegida, íntegra y disponible en todo momento.

Para el año 2017 las agencias de aduanas presentaron ante la DIAN un estimado de 1.778.000 declaraciones de importación de aproximadamente 1250 importadores y exportadores las cuales contiene información de mercancía importada o exportada, precios, proveedores en el exterior, métodos de negociación, entre otros. Esta cantidad de datos se encuentra almacenada en sistemas virtuales instalados por la DIAN, pero es responsabilidad de todos los actores en la cadena de comercio internacional mantener la data tal cual como se tiene en los sistemas informáticos.

Move Cargo S.A. mediante la consolidación de clientes rentables y la implementación de grupos de trabajo especializados para la nacionalización de productos, ha logrado un crecimiento sostenido pasando de ser una empresa pequeña a una Pyme. Dados los cambios para poder cumplir con los requisitos del crecimiento organizacional ha sido necesaria la implementación de varios software y herramientas en todos los niveles de la organización para poder prestar el servicio, lo que conlleva al aumento de la necesidad de contar con herramientas de seguridad de la información. La administración de la seguridad perimetral, el mantenimiento de los equipos, los procedimientos de Backup y el manejo de la red interna, se llevaba a cabo por un proveedor de servicios especializados contratado por la empresa, pero por decisión administrativa estas funciones deben ser asumidas por personal de la organización, quien se encargará de la protección y administración de los recursos tecnológicos.

Move Cargo está experimentando un importante crecimiento en el número de clientes y con ello se hace más evidente la necesidad de estar preparada para reaccionar de manera más rápida ante incidentes tecnológicos y adaptarse rápidamente a los cambios del entorno, los cuales son cada vez más exigentes y complejos ya que la administración de la información de los clientes debe seguir siendo, segura integra y confidencial.

Por otra parte, se han presentado eventos relacionados con la seguridad que han afectado a la organización, como pérdida la información, daño en uno de los servidores y ataque de virus. Aunque estas situaciones se han logrado resolver sin mayores perjuicios a la organización y sus operaciones, son eventos inaceptables y constituyen una voz de alerta para que se preste especial atención a la seguridad.

## 1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño de un Sistema de Gestión de Seguridad de la información (SGSI) contribuirá a mejorar la seguridad en la Agencia de Aduanas Move Cargo S.A. Nivel 1?

## 1.3 OBJETIVOS

### 1.3.1 Objetivo general

Diseñar un Sistema de Gestión de Seguridad de la información dentro de la Agencia de Aduanas Move Cargo S.A Nivel 1. Bajo la norma ISO 27001 el cual contribuya a mejorar la seguridad de la organización.

### 1.3.2 Objetivos específicos

- Determinar la situación de la empresa mediante una declaración de aplicabilidad.
- Diseñar un sistema de identificación de vulnerabilidades, evaluación y análisis de riesgos para la organización.
- Proponer las políticas, controles y sistemas de mejorar que permita el control de los riesgos y vulnerabilidades de la organización.

## 1.4 JUSTIFICACIÓN

La implementación de un SGSI dentro de los procesos de Move Cargo permite a la organización garantizar a sus clientes y partes interesadas que la información generada por prestar el servicio de desaduanamiento de mercancías no se verá afectado por factores internos o externos, y se mantendrá segura, confidencial e integra en todo momento. En el desarrollo del proyecto se logró identificar, evaluar y gestionar los riesgos, vulnerabilidades y amenazas a las que se ve expuesta ya sea por el entorno interno o el medio en el que se encuentra almacenada, permitiendo dar mejor seguridad en los procesos, así como el de evitar fallas que afecten los sistemas, la información o el servicio.

La ejecución del proyecto beneficia a la organización ya que al aplicar un SGSI diseñado, cumple con los requisitos de las partes interesadas en cuanto a la gestión de seguridad. Los clientes de Move Cargo también se ven beneficiados ya que se garantiza que la información suministrada y resultante de prestar el servicio se mantendrá confidencial, integra y disponible.

Un beneficio adicional en Move Cargo S.A es la identificación de los riesgos que podrían afectar la operacion actuando de manera preventiva ante sus causas evitando su materialización y por consecuente sus impactos.

## 1.5 ALCANCE Y DELIMITACIÓN DEL PROYECTO

El proyecto tiene como alcance el diseño de un SGSI para Move Cargo S.A. El cual se encuentra encaminado a evaluar las vulnerabilidades, amenazas y riesgos a los que está expuesta la información ya sea por factores internos o externos, lo que permitirá diseñar un sistema apropiado para los fines de la organización por medio del correcto uso de la infraestructura física y lógica, el manejo de recurso humano, el ambiente para la transferencia, los software instalados (operativo, contable y administrativo), el mantenimiento de los sistemas y el cumplimiento de la normatividad legal vigente.

El presente estudio comprende el Diseño de un (SGSI) para la Move Cargo S.A. en la ciudad de Bogotá encaminada a generar buenas prácticas en el manejo de la información basados en la norma ISO/IEC 270001.

La puesta en marcha del SGSI está fuera del alcance de este proyecto debido a que depende de la aprobación de las directivas de la organización y no de su autora, además, comprende un periodo de tiempo mucho más extenso que el de este proyecto.

# 2. MARCO DE REFERENCIA

## 2.1 ANTECEDENTE

Como guía para el desarrollo de la implementación de un Sistema de Gestión de la Seguridad de la Información en la Move Cargo S.A. Nivel 1. Se estudiaron varios proyectos que tuvieran objetivos, metodologías y resultados similares al presente proyecto, estos fueron consultados a nivel nacional e internacional y los cuales tuvieran relación directa con la seguridad informática en empresas de servicios y similares que pudiera aportar el presente proyecto.

En la Facultad de Ingeniería de la Universidad de la República en Montevideo, el ing. Gustavo Pallas Mega[1], en el año 2009, llevó a cabo un trabajo titulado "Metodología de implementación de un SGSI en un grupo empresarial jerárquico" con el objetivo de dar lineamientos metodológicos de aplicación sistemática para el diseño, implementación, mantenimiento, gestión, monitoreo y evolución de un Sistema de Gestión de Seguridad de la información según la norma ISO 27001. Entre los principales resultados obtenidos en el proyecto se destaca en análisis de riesgos utilizado ya que permitió analizar gran cantidad de riesgos director e indirectos que tiene la organización y como se logró la implementación de controles dentro de cada uno de los procesos. Este proyecto se relaciona con el presente ya que aporta ideas sobre cómo aplicar herramientas de análisis, identificación y evaluación de riesgos que permita la implementación de la norma ISO 27001 siguiendo una metodología de diseño de un Sistema de Gestión de Seguridad de la información.

En la Pontifica Universidad Católica de Perú en Lima, el Ing. Moisés Antonio Villena Aguilar[2], en el año 2006, realizó un trabajo titulado "Sistemas de gestión de seguridad de la información para una institución financiera" con el objetivo de diseñar, establecer e implementar los principales lineamientos de un modelo de sistema de gestión de la seguridad de la información la cual se encuentre alineada con el negocio, sus objetivos estratégicos y el sector en el que se desempeña. El principal resultado del trabajo es la inclusión de todos los niveles jerárquicos en la empresa para la implementación, gestión y mantenimiento del SGSI. Este proyecto aporta con el presente ya que ayuda a comprender como las necesidades y requisitos de la empresa se utilizan para diseñar el sistema para que este sea eficaz, adecuado y coherente con las estrategias del negocio.

---

[1] PALLAS, Gustavo. Metodología de implementación de un SGSI en un grupo empresarial jerárquico. Montevideo: Universidad de la república. 2009. Recuperado de: http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2-Sesion3(4).pdf

[2] VILLENA, moisés. Sistema de gestión de seguridad de información para una institución para una institución financiera: Pontificia Universidad Católica del Perú 2006. Recuperado de: http://tesis.pucp.edu.pe/repositorio/handle/123456789/362

En la Universidad Nacional Abierta y a Distancia UNAD en la ciudad de Cali – Colombia, el Ing. Luis Enrique Giraldo Cepeda[3], en el año 2016, realizo un trabajo de grado el cual se titula "Análisis para la implementación de un sistema de gestión de la seguridad de la información según norma ISO 27001en la empresas SERVIDOC S.A." con el objetivo de realizar un análisis para la implementación de un sistema que pudiera identificar y proponer soluciones de seguridad a las estaciones de trabajo que son críticas para la prestación de servicios específicamente en las áreas de contabilidad, facturación y el control de las historias críticas de la empresa, su principal resultado fue la detección de los riesgos de seguridad de la información en varios sectores que se presentan en la prestación del servicio lo que permito tomar acciones enfocadas a la mitigación, eliminación y disminución de los riesgos que se presentan en cada una de las áreas, este trabajo aporta al proyecto con ideas sobre controles de seguridad informáticos aplicables y lineamientos para establecer políticas de seguridad de la información pertinentes para algunos de los riesgos transversales para todas las empresas y vulnerabilidad más generales que se presentan en la mayoría de las organizaciones.

También en la Universidad Nacional Abierta y a Distancia UNAD, en la ciudad de Bogotá en el año 2015, la Ing. Alexandra Guzmán García en compañía del Ing. Carlos Alberto Tabora Bedoya[4], presentaron un trabajo de grado titulado "Diseño de un sistema de gestión de la seguridad de la información SGSI para empresas del área textil en la ciudades de Itagüí, Medellín y Bogotá D.C a través de la auditoria, el cual tuvo como objetivo el diseño de un SGSI basado en una auditoria aplicada en cual permita realizar un diagnóstico de la situación actual que enfrentan las Pymes del sector textil en Medellín, Itagüí y Bogotá". Como principal resultado del trabajo lograron realizar un diagnóstico del sistema de seguridad de las empresas textiles aplicando los términos de referencia de la norma ISO 27001, lo que permitió detectar las falencias y tomar acciones enfocadas a minimizar cada uno de los riesgos, este trabajo aporto al proyecto con ideas de como las necesidades y requisitos de la organización se alinean con otros sectores y empresas del país lo que permitió modelar sistemas de auditoria enfocados al cumplimiento de la norma ISO 27001.

En la Institución Universitaria Politécnico Gran Colombiano en la ciudad de Pereira – Colombia en el 2015, el Ing. Carlos Alberto Guzmán Silva[5], presento

---

[3] GIRALDO, Luis. Análisis para la implementación de un sistema de gestión de la seguridad de la información según norma ISO 27001 en la empresa SERVIDOC S.A: Universidad Nacional Abierta y a Distancia 2016, Recuperado de: http://repository.unad.edu.co:8080/bitstream/10596/6341/1/16453917.pdf

[4] GUZMAN, Alexandra y TABORA, Carlos. Diseño de un sistema de gestión de la seguridad de la información SGSI para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C. a través de una auditoria: Universidad nacional abierta y a distancia 2015, recuperado de: http://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3448/1/1030548291.pdf

[5] GUZMAN, Carlos. Diseño del sistema de gestión de seguridad de la información para una entidad financiera de segundo piso: Universidad Politécnico Gran colombiano 2015, recuperado de :

el proyecto titulado “Diseño del sistema de gestión de seguridad de la información para una entidad financiera de segundo piso” el cual tenía como propósito fundamental diseñar un SGSI acorde a las necesidades, requerimientos y expectativas de los clientes tomando como referencia la norma ISO 27001. El principal objetivo fue el diseño y la integración del mismo como un objetivo estratégico empresarial el cual mide la efectividad del sistema según parámetros de seguridad, este trabajo aporto al presente proyecto entendimiento del mecanismo para la valoración de los riesgos y la medición de los riesgos residuales después de la incorporación de los controles que eliminaran, disminuirán o transfirieran los impactos de la materialización del riesgo.

En la universidad Tecnológica de Pereira, en el año 2013, los ingenieros Juan David Aguirre Cardona en compañía de Catalina Aristizabal Betancourt [6], presentaron un proyecto titulado “Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la OFRENDA, el cual tiene como objetivo el diseñar un SGSI acorde con las necesidades y requerimientos de la organización y que resuelva los problemas actuales, el principal resultados del proyecto permitió parametrizar las estrategias y controles de seguridad en todos los niveles jerárquicos y se tomó conciencia de como la seguridad de la información es responsabilidad de todos.

## 2.2 MARCO TEORICO

### 2.2.1 Seguridad en la información

Este término hace referencia a los atributos que debe tener la información en cualquier medio para que esta tenga valor como activo. La correcta gestión de la seguridad establece que para que un activo sea seguro debe contar con los principios básicos de seguridad como lo es la confidencialidad, integridad y disponibilidad, si algún de estos tres factores falla se considera como la información no es segura[7].

Todos los sistemas de almacenamiento, tratamiento y gestión de la información se basan en mantener una integración de estos atributos los cuales se definen a continuación.

---

http://repository.poligran.edu.co/bitstream/handle/10823/654/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20%28FINAL%29.pdf?sequence=1&isAllowed=y

[6] AGUIRRE, Juan y ARISTISABAL, Catalina. Diseño de un sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda: Universidad tecnológica de Pereira 2013 recuperado de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf;jsessionid=9E2D68D87F33D77657A02A3DD7BBD7D2?sequence=1

[7] ICONTEC, Tecnología de la información vocabulario recuperado de NCT-ISO 27000.

**Confidencialidad de la información:** Son las herramientas de prevención que se tiene para prevenir que la información no se divulgada a personal o sistemas que no se encuentre autorizados. Cuando se pierde confidencialidad esta pierde valor como activo ya que la misma puede tenerla diferentes actores y esta puede ser utilizada de diferentes maneras[8].

**Integridad de la información:** este término hace referencia a como los datos se mantiene intactos, sin ningún tipo de modificación, alteración o eliminación por personal no autorizado. Cuando se pierde la integridad de la información no se puede tener certeza que el valor sea 100% correcto lo que puede afectar a la hora de usar el activo[8].

**Disponibilidad de la información:** Este atributo hace referencia a la necesidad de tener acceso al activo en el momento que el usuario o el sistema lo requiera, si se pierde la disponibilidad por mantener sistemas de seguridad robustos, el activo pierde vigencia o valor ya que no se pueden tomar acciones o decisiones de una manera más rápida[8].

### 2.2.2 El Sistema de gestión de Seguridad de la información (SGSI)

es una serie de herramientas, directrices y actividades que interactúan entre sí para dar seguridad a la información que se manipule, obtenga o elabore por medio de la relación entre una política, unos responsables definidos, unos procesos interrelacionados, unos procedimientos establecidos, recursos asignados y los sistemas utilizados para su implementación[9].

En la actualidad la protección de la información se ha convertido en uno de los aspectos más importantes para cualquier organización, ya que está es considerada como un activo intangible de gran valor y está directamente relacionado con la dirección para la toma de decisiones, evaluación de proyectos, prestación del servicio, Implementación de objetivos estratégicos, adaptación del medio económico y social, tecnología utilizadas, competencia y reglamentación aplicable.

Para la implementación SGSI se toma como base la norma ISO 27001 la cual tiene establecido la guía para adecuar los requisitos del sistema de gestión para las organizaciones lo que permite mantener un sistema adecuado, eficaz y coherente.

Para implementar un sistema de gestión de seguridad de la información eficiente y acorde con la organización se debe establecer las siguientes características.

---

[8] Blog especializados en sistemas de gestión de seguridad de la información, Confidencialidad, integridad, y disponibilidad de la información. recuperado de https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion

[9] ICONTEC, Técnicas de seguridad, sistemas de gestión de la seguridad de la información requisitos NCT-ISO 27001

- Se debe determinar el alcance del SGSI dentro de la organización teniendo en cuenta las características del negocio, el estado y los clientes.
- Establecer una política de seguridad de la información.
- Determinar un mecanismo para la evaluación y tratamiento de los riesgos internos y externos

Con la identificación de estos conceptos se puede establecer un sistema de gestión de seguridad de la información acorde y eficaz con los objetivos de la organización.

### 2.2.3 Ciclo DEMING

Siendo una norma ISO guía para la implementación del SGSI se debe tener claridad sobre los conceptos utilizados en el ciclo Deming y mejora continua ya que estos son base de todos los sistemas de calidad. El ciclo Deming consta de cuatro pasos consecuentes y consecutivos en el cual se establece los parámetros del sistema y su relación con el sistema de gestión. Los cuatro pasos se encuentran definidos de la siguiente manera[10].

**Planificación (P):** Para una correcta planificación del SGSI se debe determinar la información básica de la organización como lo es el establecimiento del contexto interno y externo en el que se desempeña la organización. En este aspecto se debe tener en cuenta los nuevos riesgos externos e internos que se puede presentar en los sistemas de información. También se debe planificar el alcance y limites que tiene el SGSI dentro de la organización por medio del establecimiento de las políticas de seguridad y los controles informáticos pertinentes.

Como parte importante del sistema se debe establecer una metodología de gestión de riesgos en el cual se identifique, evalué, controle y se haga tratamiento a los riesgos que se presente en la organización.

**Hacer (H):** En este ciclo se debe ejecutar lo planificado de la manera que fue planificada, en este aspecto es importante tener en cuenta que si se deben realizar ajustes a la planificación inicial este debe ser documentado para tener un control.

**Verificación (V):** Este ciclo valida el cumplimiento del SGSI contra los objetivos planificados y la eficacia del sistema para mantener la información disponible, integra y confidencial. El método más efectivo para validar si el sistema cumple con lo planificado es la realización de auditorías internas que validen en cumplimiento de los requisitos del sistema.

---

[10] Blog especializados en sistemas de gestión de seguridad de la información, ciclo Deming. Recuperado de https://www.pmg-ssi.com/2015/06/iso-27001-ciclo-de-deming/

**Actuar (A):** De los hallazgos detectados en la verificación se debe tomar acciones pertinentes y efectivas para que el sistema pueda cumplir con los requisitos y objetivos planificados.

Con la aplicación del ciclo Deming se establece, ejecuta y mejorar los sistemas de gestión en cualquier tipo de empresas independiente de su tamaño o sistema de producción, el ciclo Deming permite a la organización planificar de manera organizada las actividades, evaluarlas y corregirla garantizando que el sistema de gestión de seguridad de la información implementada sea funcional.

### 2.2.4 Parte del Sistema de Gestión de la seguridad de la información

Para la implementación del SGSI se deben tener claridad sobre los siguientes aspectos importantes.

**Alcance de SGSI:** En este aspecto se debe determinar hasta qué punto actúa y que limitaciones tiene el sistema de gestión de seguridad de la información dentro de la organización basado en los detalles técnicos y las actividades que realizan, para la implementación del alcance se debe tener en cuenta las el contexto tanto interno como externo en el que se desempeña o en el que se ve obligado a trabajar, las necesidades y expectativas de las partes interesadas y todas las dependencias e interfaces que se puedan presentar[11].

**Política del SGSI:** Con el alcance definido se debe determinar la política de SGSI en el cual se incluya un marco de referencia para fijar los objetivos del sistema y establecer una dirección y principios para la seguridad informática, los cuales tenga en cuenta los requisitos del negocio tanto legal como no legal y de obligaciones contractuales. La política debe estar alineada con el contexto de la organización y sus objetivos; La política debe establecer los criterios para la gestión del riesgo tanto en su identificación evaluación y control como los criterios de aceptación[12].

**Objetivos del SGSI:** La organización debe determinar los objetivos del sistema los cuales deben ser acorde con la política, debe ser medibles, cuantificables y retadores para el sistema y la organización[13].

**Implementación, operación, seguimiento y revisión de SGSI:** La organización debe planificar un plan de ruta el cual debe ser acorde con los

---

[11] Welivesecurity, Como definir el alcance del SGSI. Recuperado de: https://www.welivesecurity.com/la-es/2018/01/09/definir-alcance-sgsi/

[12] Blog especializados en sistemas de gestión de seguridad de la información, Como implementar políticas de gestión de un sistema de gestión de seguridad de la información. Recuperado de https://www.pmg-ssi.com/2014/03/iso-27001-como-implantar-politicas-de-gestion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/

[13] ICONTEC, Técnicas de seguridad, sistemas de gestión de la seguridad de la información requisitos NCT-ISO 27001

[13] ICONTEC, Técnicas de seguridad, sistemas de gestión de la seguridad de la información requisitos NCT-ISO 27001

riesgos identificados y su tratamiento definiendo las prioridades del sistema y la gestión de la operación.

También debe establecer los mecanismos de seguimiento y revisión que se deben implementar en el SGSI, determinado el grado de cumplimiento de los objetivos planificados y su eficiencia[13].

**Requisitos de documentación:** La organización debe determinar los mecanismos para documentar los procedimientos, formatos, informes, resultados y demás documentación relacionada con el SGSI, en un sistema el cual se encuentre disponible, seguro y confidencial para las partes interesadas. La organización debe diseñar un sistema de control de documentación y de registros que asegure la vigencia y fiabilidad de la documentación[13].

**Compromiso de la dirección:** La dirección debe garantizar el compromiso con el SGSI aprobando la política de calidad, los objetivos y haciéndolos cumplir en todos los niveles de la organización. La dirección también debe establecer las funciones y responsabilidades en cuanto al Sistema de Gestión de Seguridad de la Información y realizando la revisión por la dirección sobre los resultados del sistema[13].

**Gestión de recursos:** La dirección debe suministrar los recursos económicos, humanos y tecnológicos necesarios para poder ejecutar los procedimientos del SGSI en el cual incluye los recursos para que el personal encargado del sistema tenga los conocimientos, la formación y la competencia necesaria para poder gestionar de manera efectiva el sistema[13].

**Auditorías internas del SGSI:** Después de la ejecución de la planificación del sistema se debe ejecutar un plan de auditoria interna en el cual se verifiquen si se están cumpliendo los requisitos establecidos, estas auditorías debe ser realizadas en periodos planificados por personal capacitado. La ejecución de la auditoria interna tiene como finalidad el de determinar si el sistema tiene un desempeño acorde con lo esperado[13].

**Revisión por la dirección:** La dirección de la organización debe determinar si el SGSI está acorde con la organización y sus requisitos revisando la siguiente información relacionada[13]:

- Resultados de la auditoria interna y revisión del SGSI
- Retroalimentación de las partes interesadas
- Estados de las acciones correctivas y preventivas
- Vulnerabilidades o amenazas no tratadas adecuadamente
- Resultado de las mediciones de eficacia
- Cualquier cambio que pudiera afectar el SGSI
- Recomendaciones para la mejora

Como resultado de esta revisión se tendrá:

- ❖ Plan para la mejora de la eficacia
- ❖ La actualización de evaluación de riesgos y del plan de tratamiento
- ❖ La modificación de procedimiento y controles que afecten la seguridad de la información
- ❖ La identificación de cambios en los requisitos y el contexto de la organización
- ❖ La identificación de los recursos necesarios para el mantenimiento del SGSI

**Mejora del SGSI:** La organización debe tomar acciones sobre los resultados no deseados o fallas en el sistema por medio de acciones correctivas para así poder atacar las causas fundamentales del problema garantizando que estas no vuelvan a ocurrir. También deben tomar acciones contra efectos no deseados potenciales para que así estos no se materialicen[13].

### 2.2.5 Gestión del riesgo en la seguridad informática

Es una metodología utilizada para identificar posibles riesgos y amenazas que tiene el sistema informáticos y que pudieran afectar de manera parcial o total la información, la infraestructura tecnológica, las herramientas de comunicación o el software utilizados para cualquier negocio[14].

La gestión de riesgo tiene varias metodologías para identificar, evaluar y controlar los riesgos, pero para el proyecto utilizaremos el especificado para el sistema de gestión de seguridad de la información en el cual se valoran diferentes factores e impactos y así poder diseñar los controles pertinentes para minimizar, eliminar, transferir o aceptar el impacto de los riesgos.

Para realizar un análisis de riesgos informáticos acorde con el tamaño y necesidades de la organización se deben seguir los siguientes pasos:

**Análisis de riesgos cualitativo:** En este aspecto se evalúa la importancia de cada uno de los activos del sistema de gestión de seguridad de la información que se presentan en la organización y el impacto que este tendría dentro de la organización si fuera afectado parcial o totalmente. Esta valoración se realiza evaluando cada aspecto de seguridad.

**Identificación de riesgos, vulnerabilidades y amenazas:** En este aspecto se realiza una identificación de los posibles factores que pudieran afectar la información o los sistemas, estos factores se encuentran agrupados y se realiza valoración por cada uno.

---

[13] ICONTEC, Técnicas de seguridad, sistemas de gestión de la seguridad de la información requisitos NCT-ISO 27001

[14] Gestión de riesgo en la seguridad informática, análisis de riesgo recuperado de: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

En este aspecto se valora cada uno de los riesgos contra cada uno de los activos y como esta afecta o degrada los atributos de la información.

**Valoración de vulnerabilidad y nivel de riesgo:** Después de identificar cada uno de los riesgos, vulnerabilidades y amenazas que pueden afectar a la información se realiza una valoración del nivel de probabilidad de que el evento en cuestión ocurra y el impacto que este generaría. De la valoración de estos aspectos se determina un nivel de riesgo para ser tratado[15].

**Control de riesgos:** de la valoración de los riesgos se diseñan controles, políticas, parámetros o restricciones para tratar cada uno de las causas del riesgo con el fin de minimizar, eliminar, transferir o aceptar el impacto de la materialización de los riesgos.

**Gestión del riesgo:** La organización debe determinar los criterios y metodologías para identificar, evaluar y valorar el riesgo a los que se ve expuesto por el medio en el que se desempeña y las características de la empresa[16].

También se debe identificar los mecanismos para el tratamiento de los riesgos y la evaluación de tratamiento y aceptación.

### 2.2.6 Vulnerabilidad informática

Son consideradas como las posibilidades de que ocurra un evento que ponga en riesgo la información, la infraestructura física o lógica utilizada para administrar la seguridad. Existen varios tipos de vulnerabilidad a los cuales siempre se está expuesto, pero aplicando una correcta administración de recursos los impactos de las vulnerabilidades son disminuidos.

Existen varios tipos de vulnerabilidades que pueden afectar los SGSI como son[17]:

**Vulnerabilidad física:** son aquellas que son ocasionadas por las debilidades o falencias que existen en el entorno físico que puedan afectar a los computadores, equipos de comunicación, servidores o redes que permitan ataques o hurtos.

**Vulnerabilidad natural:** son los eventos naturales de cualquier tipo que ocasione una vulnerabilidad en el sistema o que permita acceso a información.

**Vulnerabilidad Humana:** son aquellas que por falta de conocimientos o actos malintencionadas afecten de manera negativa a los medios o

[15] Magerit, Libro III – Catalogo de elementos
[16] Magerit, Libro I – Catalogo de elementos
[17] Magerit, Libro II – Catalogo de elementos

elementos de protección de la información, dejando vulnerabilidades, amenazas o riesgos.

**Vulnerabilidades de Hardware**: es la posibilidad que uno de los equipos o piezas físicas de la infraestructura presente alguna falla en su funcionamiento ya sea por el mal uso, desperfectos de fábrica o por mala manipulación.

**Vulnerabilidades de software**: Son aquellas vulnerabilidades del software que permite acceder a los sistemas, configuración o información de los equipos con pocas o ninguna medida de restricción ya sea por falta de configuración, errores en el código fuente o vulnerabilidades conocidas.

**Vulnerabilidades de dispositivos móviles**: se dan cuando por errores en la configuración, daños o descuidos un tercero puede extraer o robar información de los equipos por medio de dispositivos móviles como USB o memorias de cómputo.

**Vulnerabilidad económica**: se presenta cuando no existe los suficientes recursos para mantener y mejorar un sistema de seguridad adecuado para mantener la información protegida.

### 2.2.7 Amenazas informáticas

Las amenazas informáticas son consideradas como la posibilidad que algún evento pueda realizar un daño a la infraestructura o a la información almacenada, existen varios tipos de amenazas los cuales son[15]:

**Amenazas naturales**: Son aquellos eventos naturales que de ocurrir generarían un impacto negativo en la infraestructura del sistema, la información almacenada o los medios de seguridad implementados, los tipos de amenazas naturales son

- Fenómeno Climático.
- Fenómeno Sísmico.
- Fenómeno de origen volcánico.
- Fenómeno meteorológico.
- Inundación.

**Amenazas Industriales:** Son aquellos eventos en los cuales la infraestructura determinada para proteger la información falla generado amenazas como lo son.

- Fuego.
- Daños por agua.
- Explosiones.
- Sobrecarga eléctrica.

- Contaminación mecánica (Polvo, vibración, suciedad, etc.)
- Avería de origen físico o lógico.
- Corte de suministro eléctrico.
- Condiciones inadecuadas de temperatura o humedad.
- Fallo de servicio de comunicación (Internet, Teléfono. Etc.).
- Interrupción de servicios esenciales.
- Degradación de soportes de almacenamiento de la información.

**Amenazas internas:** Las amenazas internas se presentan cuando los administradores o usuarios de sistemas con intención o sin ella generan un posible fallo o vulnerabilidad en los sistemas que pudieran afectar a los equipos o a la información contenida en ella. Algunos de las amenazas son:

- Errores de usuario.
- Errores de administrador.
- Errores de monitorización.
- Errores de configuración.
- Difusión de software dañino.
- Escapes de información.
- Alteración accidental de la información.
- Destrucción de la información.
- Fugas de información.
- Errores de mantenimiento / actualización de programas (software).
- Errores de mantenimiento / actualización de equipos (hardware).
- Perdida de equipos.
- Indisponibilidad del personal.

**Amenazas Externas:** Son aquellas amenazas de origen externo a la compañía de la cual no se tiene control y puede afectar la infraestructura física o a la información almacenada en ella.

- Manipulación de los registros de actividad.
- Manipulación de la configuración.
- Suplantación de la identidad del usuario.
- Abuso de privilegios de acceso.
- Difusión de software dañino (malware).
- Re encaminamiento de mensajes.
- Alteración de secuencia.
- Acceso no autorizado.
- Modificación deliberada de información.
- Destrucción de información.
- Divulgación de información.
- Manipulación malintencionada de equipos.
- Robo.
- Ataque destructivo.
- Ingeniería social

### 2.2.8 Gobierno TI

El Gobierno de TI es parte integral del Gobierno Corporativo y consiste en el liderazgo, estructura organizacional y procesos que aseguran que las Tecnologías de Información de una organización estén alineadas y acorde a las estrategias y objetivos de la misma[18].

El gobierno de TI o llamado también gobernabilidad de TI es responsabilidad de la junta de directores y gerencia de una organización. En medio de las responsabilidades del gobierno de TI como son establecer estrategias, administrar riesgos y medir desempeño. Un factor primordial para el éxito de estas estructuras y procesos es una adecuada comunicación de todas las partes involucradas, basadas en relaciones constructivas, un lenguaje común y un compromiso compartido.

Las responsabilidades del gobierno de TI forman parte del gobierno corporativo y deben ser conducidas como cualquier otra estrategia. En términos más sencillos, el gobierno debe ser efectivo, transparente y medible.

### 2.2.9 Legislación aduanera

Está legislación está conformada por un sistema estructurado y lógico de Ley, decretos, resoluciones, circulares y normas relacionadas en los tratados de libre comercio, cuyo alcance es reglamentar y controlar el comercio exterior colombiano[19].

La legislación aduanera está dada por Decretos, Resoluciones y Circulares enfocados prioritariamente al ajuste de procedimientos para que este se encuentre alineados con los lineamientos y directrices de la Organización Mundial de Aduanas-OMA, la Organización Mundial del Comercio OMC, los Tratados de Libre Comercio y la realidad económica, comercial y estructural de la sociedad.

Dentro de este marco normativo, los regímenes aduaneros son el tratamiento que se les debe dar a las mercancías para ser sometidos a control y vigilancia por medio de la autoridad aduanera, mediante el cual se asigna un destino específico relacionado al comercio internacional y este se encuentre conforme con las normas aduaneras. Actualmente estos regímenes son: la importación, la exportación, régimen de depósito aduanero y el de tránsito aduanero[20].

Para cumplir con los requisitos aduaneros, la DIAN ha implementado un sistema Informático que permiten a los usuarios del comercio exterior intercambiar información con la DIAN y hacer sus trámites de manera virtual.

---

[18] Gobierno IT. Arquitectura IT Colombia recuperado de: http://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8078.html

[19] Sánchez Julia, Nueva regulación aduanera en Colombia aspectos didácticos.

[20] Ministerio de hacienda y crédito público- Decreto 390 regulación aduanera

En atención a lo anterior, la mayoría de los trámites de la importación ordinaria, como la modalidad de importación, se realizan a través de los servicios informáticos electrónicos ingresando a la página Web de la DIAN, sin embargo se evidencia que aunque se ha avanzado en este propósito, los trámites aduaneros dada la complejidad que encierra la nacionalización de mercancías de procedencia extranjera requieren de la intervención de los Operadores de Comercio Exterior, como lo son las Agencias de Aduana.

Las Agencias de Aduana cumplen un papel preponderante en la operaciones de comercio exterior, al punto que son las encargadas de declarar las mercancías ante la DIAN a través de los sistemas informáticos electrónicos, es decir, suscriben y presentan la declaración de mercancías a nombre propio o por encargo de terceros, cuyo acto consiste en la indicación del régimen aduanero que ha de aplicarse a las mercancías y en consignar los elementos e Informaciones exigidos por la normatividad aduanera vigente en un documento que se denomina declaración de importación.

### 2.2.10 Agencias de Aduanas

Son persona jurídica autorizada por la Dirección de Impuestos y Aduanas Nacionales para prestar servicios de representación a los importadores, exportadores o declarantes para realizar los trámites aduaneros correspondientes. En ejercicio de su autorización, podrán desarrollar las actividades relacionadas con el agenciamiento aduanero, actividad de naturaleza mercantil y de servicio, orientada a garantizar que se cumpla con la legislación aduanera y de comercio exterior vigentes y con cualquier trámite o procedimiento para la adecuada aplicación de los destinos aduaneros, incluidos los regímenes aduaneros[21].

Como novedad especial, la nueva legislación, elimina la obligatoriedad de la utilización de la agencia de aduanas para realizar el desaduanamiento de las mercancías, al determinar que los importadores, los operadores del régimen de envíos de entrega rápida o mensajería expresa y el operador postal oficial de correos pueden actuar directamente ante la autoridad aduanera para realizar sus propios trámites.

Los agentes económicos intervinientes en el proceso de importación participan según el desarrollo propio de su actividad económica en virtud del principio de la iniciativa privada y libertad económica constitucional; no obstante, dado el control del ejecutivo conforme con las normas citadas, es importante señalar que éstos requieren de autorización o habilitación para ejercer dicha actividad con el cumplimiento de unos requisitos, con obligaciones preestablecidas y sanciones por el incumplimiento de las mismas conforme con el principio de legalidad, señaladas en el Decreto 2685 de 1999, y en tránsito de sustitución por las nuevas normas contenidas en el Decreto 390 de 2016:

[21] Ministerio de hacienda y crédito público - Decreto 390. Sección 1, articulo 54 Agencias de aduanas

- ✓ Entre los procesos de importación intervienen los siguientes actores:
- ✓ Autoridad Aduanera –DIAN –
- ✓ Entidades de Control (ICA, INVIMA, MINSALUD, INDUMIL, etc.)
- ✓ Importador
- ✓ Transportista internacional
- ✓ Agencia Naviera
- ✓ Agente de Carga
- ✓ Puertos, aeropuertos y sociedades portuarias
- ✓ Agencia de Aduanas
- ✓ Depósito Aduanero
- ✓ Transportador nacional

Cada uno de los anteriores actores tiene definición legal, funciones, responsabilidades y régimen sancionatorio en el decreto 390 de 2016 cuya vigencia es escalonada en 3 etapas, la primera etapa entró en vigencia el pasado 23 de marzo de 2016.

Move Cargo en su planeación estratégica de mediano plazo, previo el análisis del entorno, decidió emprender acciones para asegurar que la información de la organización se encuentre segura contra los factores externos e internos que pudieran afectarla.

## 2.3 MARCO CONTEXTUAL

**Razón Social:** Agencia de Aduanas Move Cargo S.A Nivel 1
**Ubicación:** Carrera 102 A # 25H – 45 Oficina 201. Bogotá – Colombia
**Reseña Histórica:** La ***AGENCIA DE ADUANAS MOVE CARGO S.A NIVEL 1*** (en adelante "***MOVE CARGO*** ") fue fundada en 1994 por el señor German Fajardo para prestar los servicios de agenciamiento aduanero en cumplimiento de las normas legales vigentes.

Desde su fundación comienza operaciones en el campo del comercio internacional ofreciendo sus servicios de desaduanamiento de mercancías, operando en su sede Bogotá. En el año 2007 nace **Move Cargo** *Cartagena* para cubrir las necesidades de agenciamiento aduanero de los clientes en el Atlántico Colombiano y en el año 2010 nace **Move Cargo** Buenaventura cubriendo las necesidades de agenciamiento de los clientes en el pacífico.

Como logro a su trayectoria se encuentra autorizada para actuar como Agencia de Aduanas Nivel 1, lo que le permite realizar trámites en todas las administraciones de Colombia aplicando los diferentes regímenes aduaneros de importación y exportación.

Gracias a su crecimiento sostenido a través de los años, implementó varios departamentos con el fin de controlar las operaciones. Uno de estos

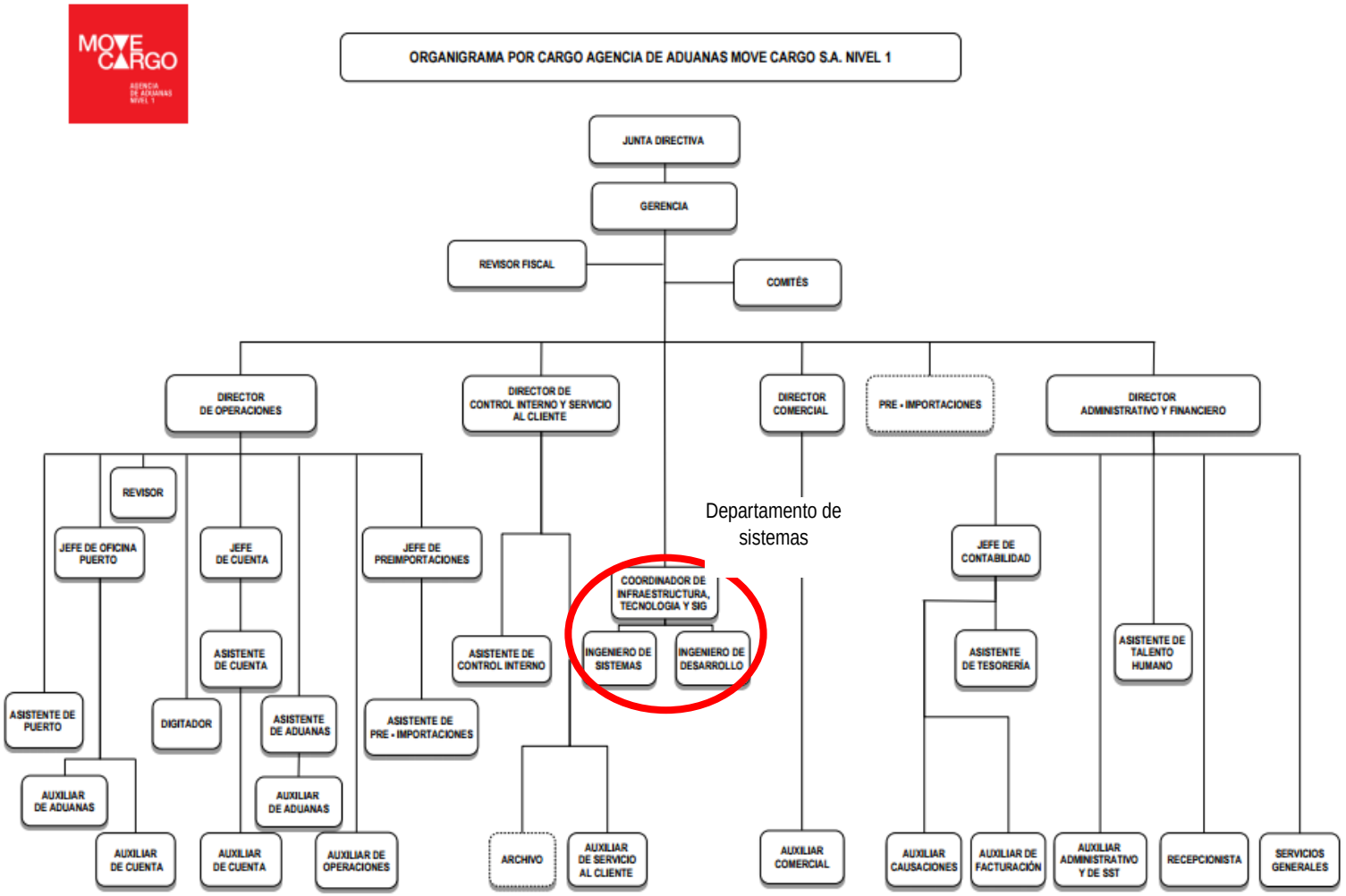
departamentos es el área de tecnología la cual consta de un ingeniero de sistema dedicado al mantenimiento, configuración y administración de los sistemas de seguridad, un ingeniero de desarrollador encargado de generar herramientas tecnológicas a todas las áreas de la organización en herramientas libres y un coordinador encargado de administrar los sistemas informáticos tal y como se muestra en la figura 1.

El departamento tiene el objetivo de mantener la infraestructura tecnológica de la organización y hace parte fundamental del mapa de procesos como se muestra la figura 2. La estructura tecnología implementada consta de 60 equipos de cómputo fijos, 6 portátiles, 4 servidores físicos y 8 virtuales como se muestra en la figura 3.

Se cuenta con desarrollos propios, software administrativo, contable y operativo que se integran para prestar el servicio de agenciamiento aduanero, este software es contratados con proveedores externos que garantizan su funcionalidad, mantenimiento y actualización. Se tiene contratado con un proveedor externo para realizar mantenimientos preventivos a la infraestructura informática, la cual se realiza en periodos planificados y la administración de seguridad perimetral contra intrusos o malware que afecte la operación.

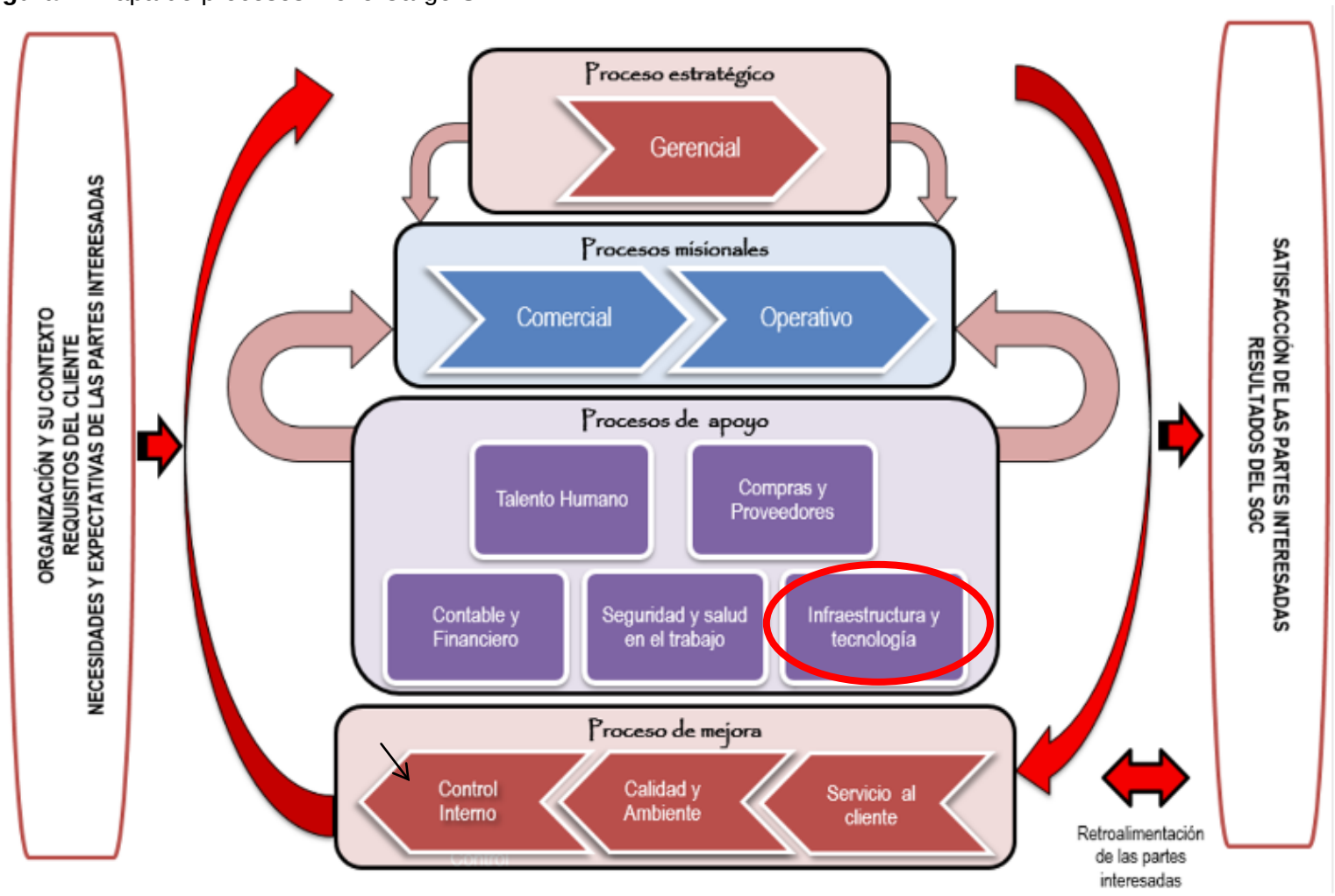
La gerencia determino el objetivo específico al grupo de ingeniería, así como las actividades puntuales, los medios de control, así como medios de medición y verificación del sistema.

**Figura 1**. Organigrama de la agencia de aduanas Move Cargo S.A.



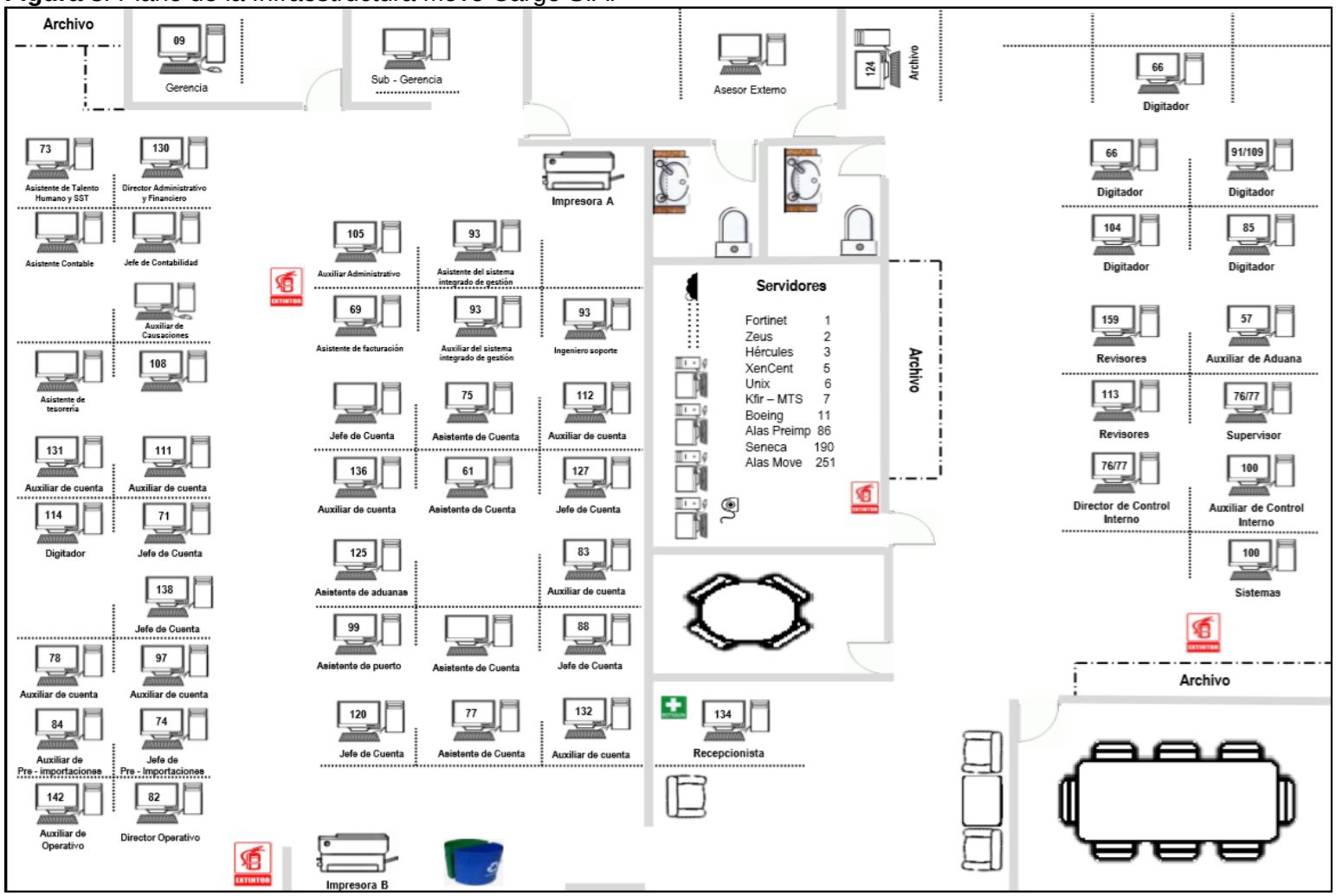

**Fuente:** https://movecargo.darumasoftware.com/frontend_movecargo.php

**Figura 2**. Mapa de procesos Move Cargo S.A.




**Fuente:** https://movecargo.darumasoftware.com/frontend_movecargo.php

**Figura 3**. Plano de la Infraestructura Move Cargo S.A.




**Fuente:** https://movecargo.darumasoftware.com/frontend_movecargo.php

El objetivo del proceso de infraestructura y tecnología es proteger la información y la infraestructura física y digital por medio de herramientas de seguridad, protocolos y controles que garanticen que siempre se encuentre disponible, integra y confidencial.

## 2.4 MARCO LEGAL

Colombia como país productivo y con base para el impulso de la economía y el bienestar de la sociedad ha implementado modelos productivos basados en la prestación, venta y comercialización de productos y servicios a nivel nacional e internacional, soportados por herramientas tecnológicas para el control y la administración de los negocios, siendo la tecnología un factor importante para la productividad del país y preocupados por el uso indebido de estas tecnologías el gobierno nacional crea el ministerio de las tecnologías de la información y comunicaciones para regular el uso.

El gobierno nacional expidió varias normas de seguridad informática para los sectores más críticos de la economía como lo es el financiero y de este parte para los demás sectores, en la actualidad tener sistemas de seguridad informáticos y el buen uso de este está protegido y reglamentado obligando a Move Cargo a implementar modelos de seguridad y control que permite cumplir a cabalidad con todas las normas aplicables al sector productivo o sector de la economía. A continuación, se menciona la reglamentación aplicable, la cual es base para la implementación de un modelo de seguridad informática. Uno de los principales aspectos legales para la prestación del servicio de agenciamiento aduanero es la alienación de la organización con la estratégica del gobierno en línea de la república de Colombia conferido en el decreto 1151 del ministerio de comunicaciones, o el decreto 1747 de 2000 sobre la reglamentación de los certificados y firmas digitales utilizados por la organización.

Otras reglamentaciones aplicables a la organización y son tenidas en cuenta en el presente proyecto es la protección de *habeas data* de la cual la organización tenga conocimiento o manipule para la prestación del servicio o administración del negocio determinado en la circular No .02 de 2015 emitida por la superintendencia de industria y comercio. Todas las actividades en materia de protección de la información y los datos esta alineadas con los artículos del código penal y cuáles son las acciones sancionadas penales por la mala utilización de los mismo descritos en la ley 1273 de 5 de enero del 2009

# 3. METODOLOGÍA

## 3.1 TIPO DE INVESTIGACIÓN

Este proyecto se llevó a cabo bajo el enfoque Cuantitativo, aplicando un estudio de tipo descriptivo, donde se analizó el estado actual de la organización en cuanto a la seguridad de la información usando herramientas y metodologías aplicadas en la actualidad y con base en ello se propuso, más no se implementó, controles y políticas para mejorar dicha seguridad.

## 3.2 DISEÑO DE INVESTIGACIÓN

El Sistema de Gestión de Seguridad de la Información para la agencia de Aduanas Move Cargo S.A Nivel 1 se diseñó aplicando la norma ISO 27001, que considera las siguientes fases:

**1. Requisitos generales**
Se debe determinar cuáles con los requisitos indispensables y obligatorios que debe cumplir el sistema de gestión de seguridad de la información teniendo en cuenta el contexto tanto interno como externo de la organización.

El establecimiento del contexto de la organización tiene en cuenta factores como los socios del negocio, los empleados, las directicas, los clientes y todas las partes interesadas del negocio para así poder determinar de una manera más clara los requisitos del sistema. Con los requisitos y el contexto de la organización definido se identifican los riesgos que pudieran afectar el cumplimiento de estos requisitos, se debe determinar sus causas y el nivel de riesgo que tiene cada una.

**2. Establecimiento y gestión del SGSI**
**Alcance de SGSI**
El alcance para Move Cargo S.A. Es la protección de la información que genera, maneja y manipula protegiendo los medios en los que se elabora, almacena y protege.

**Política del SGSI**
La dirección determina la política teniendo como precedente el contexto interno y externo de la organización, el servicio que presta, la reglamentación aplicable y los requisitos y necesidades de las partes interesadas.

**Gestión del riesgo**
Para la gestión de riesgos la organización utiliza herramientas que permiten la identificación de riesgos en la que la organización se ve expuesta teniendo en

cuenta el medio en el que desempeña, las características de la empresa y el servicio que presta.

**Objetivos del SGSI**
Con la política implementa la dirección determinar los objetivos del sistema los cuales están alineados con la política, son medibles y coherentes con el negocio.

**3. Requisitos de documentación**
La organización determina que para que el sistema se documente de una manera efectiva se alinearan con los parámetros establecidos en el sistema de calidad implementado el cual está acorde con los requisitos de la norma ISO 9001:2015. Toda la documentación de SGSI será identifica, documenta y almacenada como se establece en los parámetros de la organización.

**Compromiso de la dirección**
La dirección realiza seguimientos periódicos al SGSI para garantizar que este sea eficiente, adecuado y conveniente para la organización y su propósito.

**Gestión de recursos**
Se determina los recursos para la implementación, mantenimiento y mejora del SGSI en Move Cargo S.A. Por medio de la elaboración de un presupuesto de gastos elaborado por la dirección.

**4. Auditorías internas del SGSI**
Como parte integral del sistema, se planifica auditorías al sistema dirigidas por personal interno capacitado para validar el cumplimiento de los requisitos especificados por la norma ISO 27001, la organización y las partes interesadas.
Estas auditorías dejan registro y los hallazgos detectados deben ser tratados por los responsables.

**5. Revisión del SGSI por la dirección**
La dirección de la organización por medio de la revisión de los resultados determina si esta es acorde, eficaz y adecuada para la organización y su propósito, la dirección evalúa por medio de la revisión de:

- Resultados de la auditoria interna y revisión del SGSI.
- Retroalimentación de las partes interesadas.
- Estados de las acciones correctivas y preventivas.
- Vulnerabilidades o amenazas no tratadas adecuadamente.
- Resultado de las mediciones de eficacia.
- Cualquier cambio que pudiera afectar el SGSI.
- Recomendaciones para la mejora.

Como resultado de esta revisión la dirección debe determinar:

- Plan para la mejora del SGSI.
- La actualización de la gestión de riesgos y plan de tratamiento.
- La modificación de procedimiento y controles que afecten la seguridad de la información.
- La identificación de cambios en los requisitos y el contexto de la organización.
- La identificación de los recursos necesarios para el mantenimiento del SGSI.

# 4. RESULTADOS

## 4.1 DECLARACIÓN DE APLICABILIDAD

En esta fase del proyecto se relacionarán los controles de la norma ISO 27001: 2013 determinado cuales son aplicables teniendo en cuenta el contexto en el que se desempeña, el servicio que presta, la reglamentación aplicable, los requisitos y necesidades de las partes interesadas.

La primera actividad consistió en hacer un inventario de los activos de la organización, los cuales se relacionan a continuación:

### 4.1.1 Inventario de activos

**Activos de software**

Software contable - Informa web
Software operativo - ALAS, PREIMPO y CUSTOMSGM
Software de gestión - DARUMA
El software instalado tiene mantenimiento continuo con el proveedor por medio de tickets o solicitudes de servicio, se garantiza disponibilidad del software el 99% del tiempo.
Software propio - Gincomex, Automove y Clasificador arancelario.
El software propio es administrado y soportado por el área de infraestructura el cual tiene los conocimientos y permisos para manipular los códigos.

**Activos de hardware (Servidores físicos y virtuales)**

- Servidor XENSERVER
- Servidor Fortinet
- Servidor ZEUS
- Servidor INFORMAWEB
- Servidor Asterisk
- Servidor Custom - Sinergia
- Servidor ALAS PREIMPO
- Servidor ALASMOVE 2
- Servidor MTS
- Servidor BOEING
- Servidor SENECA
- Servidor Cámaras
- Impresora A
- Impresora B
- 60 equipos fijos
- 6 Portátiles
- UPS

**Redes de comunicación**

Actualmente la organización cuenta con una planta telefónica con 45 líneas de teléfonos fijos, Un sistema de correos electrónicos contratados con un proveedor con 100 cuentas de usuarios, cada puesto de trabajo fijo cuenta con punto para acceso a Internet y los portátiles con redes inalámbricas.

**Instalaciones**

La organización cuenta con instalaciones propias ubicadas en el edificio del aeropuerto en la carrera 102 A No 25H – 45 Oficina 201, la empresa comparte las instalaciones del edificio con aproximadamente otras 10 empresas del mismo sector.

**Intangibles**

La organización ha determinado que el almacenamiento de la información de todas las áreas se realice con la infraestructura propia y sea protegida por el departamento de infraestructura y tecnología, por normatividad vigente esta debe ser protegida, almacenada y disponible durante 20 años a partir de la creación del documento y su presentación ante entes gubernamentales.

La información resultante de la prestación de servicio de agenciamiento aduanero es considerada como uno de los bienes intangibles más importantes ya que la información resultado de la prestación del servicio es tomada para realizar otras operaciones y alimenta la base de datos de la organización.

### 4.1.2 Declaración de aplicabilidad para la Move Cargo.

Se emite la presente declaración de aplicabilidad para (SGSI) de Move Cargo S.A.

**Cuadro 1.** Declaración de aplicabilidad

| Declaración de aplicabilidad | | | | |
|---|---|---|---|---|
| **A5** | | **Políticas de la seguridad de la información** | | |
| **A5.1** | | **Orientación de la dirección para la gestión de la seguridad de la información** | | |
| | A5.1.1 | Políticas para la seguridad de la información | Aplica | Se cuenta con una política de seguridad de la información para el SGSI, aplicada a todos los cargos en la cual se tiene en cuenta los parámetros de seguridad informática dentro de la de organización |

**Cuadro 1.** (Continuación)

| Declaración de aplicabilidad | | | | |
|---|---|---|---|---|
| | A5.1.2 | Revisión de las políticas para la seguridad de la información. | Aplica | Anualmente la dirección revisa la política de seguridad para adecuarla a las necesidades y aspectos de la organización.<br><br>Para tener una política actualizada la dirección en conjunto con el departamento de tecnología verifica el contexto externo de la organización para verificar cuales son las amenazas existentes. |
| **A6** | | **Organización de la seguridad de la información** | | |
| **A6.1** | | **Organización interna** | | |
| | A6.1.1 | Roles y responsabilidades para la seguridad de la información | Aplica | Se cuenta con perfiles de cargo, procesos, protocolos y responsables para mantener el sistema de seguridad informática.<br><br>Es deber de la gerencia, los dueños de procesos y el procesos de tecnología implementar, mantener y divulgar las políticas de seguridad informática |
| | A6.1.2 | Separación de deberes | Aplica | Se cuenta con departamentos responsables de la seguridad tanto física como digital. |
| | A6.1.3 | Contacto con las autoridades | Aplica | Se cuenta con protocolos de comunicación en caso de emergencia o cuando se vea comprometida la información. |
| | A6.1.4 | Contacto con grupos de interés especial. | Aplica | Se cuenta con un protocolo de comunicación externa con todos las partes interesadas. |
| | A6.1.5 | Seguridad de la información en la gestión de proyectos. | No Aplica | No se realizan proyectos informáticos. |
| **A6.2** | | **Dispositivos móviles y teletrabajo** | | |
| | A6.2.1 | Política para dispositivos móviles | Aplica | Se cuenta con medidas de seguridad para administrar los dispositivos móviles |
| | A6.2.2 | Teletrabajo | No Aplica | Debido a las características de la empresa y el servicio prestado no se maneja esta modalidad |

**Cuadro 1.** (Continuación)

| Declaración de aplicabilidad | | | | |
|---|---|---|---|---|
| **A7** | | **Seguridad de los recursos humanos** | | |
| **A7.1** | | **Antes de asumir el empleo** | | |
| | A7.1.1 | Selección | Aplica | Se especifica las características del empleado que manejara el sistema de seguridad (Experiencia, estudios, habilidades) |
| | A7.1.2 | Términos y condiciones del empleo | Aplica | La empresa cuenta con contratos a términos indefinidos para mantener al personal. |
| **A7.2** | | **Durante la ejecución del empleo** | | |
| | A7.2.1 | Responsabilidades de la dirección | Aplica | La dirección está comprometida con el sistema de seguridad de la información por medio de la implementación de políticas y procedimientos. |
| | A7.2.2 | Toma de conciencia, educación y formación en la seguridad de la información. | Aplica | Se cuenta con programas de capacitaciones, inducción y sensibilización a los empleados con temas relacionados en seguridad. |
| | A7.2.3 | Proceso disciplinario | Aplica | Se cuenta con un reglamento disciplinario para los eventos relacionados con la seguridad, para los casos más graves se aplica los establecidos por la ley. |
| **A7.3** | | **Terminación y cambio de empleo** | | |
| | A7.3.1 | Terminación o cambio de responsabilidades de empleo | Aplica | Se aplican las actividades establecidas en los procedimientos de personal. |
| **A8** | | **Gestión de activos** | | |
| **A8.1** | | **Responsabilidad por los activos** | | |
| | A8.1.1 | Inventario de activos | Aplica | Se cuenta con el control de todos los activos de la organización necesarios para la prestación del servicio |
| | A8.1.2 | Propiedad de los activos | Aplica | La empresa no cuenta con activos propios, Todos son contratados a un tercero. |
| | A8.1.3 | Uso aceptable de los activos | Aplica | Todos los activos son verificados y probados por el departamento de sistemas antes de su implementación y utilización. |
| | A8.1.4 | Devolución de activos | Aplica | El departamento comercial cuenta con las herramientas y contratos necesarios para realizar devolución o cambios por garantías. |

**Cuadro 1.** (Continuación)

| Declaración de aplicabilidad | | | | |
|---|---|---|---|---|
| **A8.2** | | **Clasificación de la información** | | |
| | A8.2.1 | Clasificación de la información | Aplica | La información se encuentra clasificada según su importancia y necesidad para la prestación del servicio |
| | A8.2.2 | Etiquetado de la información | Aplica | Se cuenta con protocolos de cómo se debe realizar la manipulación de las bases de datos y la información confidencial. |
| | A8.2.3 | Manejo de activos | Aplica | Todos los activos mantienen una documentación adecuada para su manejo |
| **A8.3** | | **Manejo de medios** | | |
| | A8.3.1 | Gestión de medios removibles | Aplica | En los equipos operativos y administrativos esta opción se encuentra bloquead por política. |
| | A8.3.2 | Disposición de los medios | Aplica | Los medios removibles son utilizados y manejados por la gerencia y los directivos. |
| | A8.3.3 | Transferencia de medios físicos | No Aplica | Esta actividad no se realiza dentro de la organización |
| **A9** | | **Control de acceso** | | |
| **A9.1** | | **Requisitos del negocio para el control de acceso** | | |
| | A9.1.1 | Política de control de acceso | Aplica | Se cuenta con sistemas de seguridad y control de acceso a la oficina y controles adicionales para el acceso al cuarto de sistemas. |
| | A9.1.2 | Acceso a redes y a servicios en red | Aplica | Se cuenta con una política de acceso a internet en la cual se tiene bloqueado la entrada a sitios de música, videos y medios de descarga. |
| **A9.2** | | **Gestión de acceso de usuarios** | | |
| | A9.2.1 | Registro y cancelación del registro de usuarios | Aplica | Se cuenta con procedimientos para la desactivación de claves y permisos en el sistema. |
| | A9.2.2 | Suministro de acceso de usuarios | Aplica | Siguiendo los parámetros de perfiles y talento humano, se habilitan los permisos necesarios y suficientes a cada usuario para realizar la labor designada. |
| | A9.2.3 | Gestión de derechos de acceso privilegiado | Aplica | Cada perfil tiene establecido los privilegios que necesita para desarrollar su labor. |

**Cuadro 1.** (Continuación)

| Declaración de aplicabilidad | | | | |
|---|---|---|---|---|
| | A9.2.4 | Gestión de información de autenticación secreta de usuarios | Aplica | Todos los cargos cuentan con usuarios para autenticarse en los sistemas informáticos de la organización |
| | A9.2.5 | Revisión de los derechos de acceso de usuarios | Aplica | Cada cargo cuenta con la descripción de accesos necesaria y suficiente para realizar su labor. |
| | A9.2.6 | Retiro o ajuste de los derechos de acceso | Aplica | Como protocolo de seguridad los empleados retirados se deshabilita todos los acceso de manera inmediata. |
| **A9.3** | | **Responsabilidades de los usuarios** | | |
| | A9.3.1 | Uso de información de autenticación secreta | Aplica | Se cuenta con políticas para el manejo de la información confidencial o sensible. |
| **A9.4** | | **Control de acceso a sistemas y aplicaciones** | | |
| | A9.4.1 | Restricción de acceso a la información | Aplica | Se cuenta con políticas de manejo de la información y solo cargos de confianza puede manipularla. |
| | A9.4.2 | Procedimiento de ingreso seguro | Aplica | Cada usuario debe ingresar a las terminales con sus claves de acceso designadas para dicho fin. |
| | A9.4.3 | Sistema de gestión de contraseñas | Aplica | Se cuenta con un sistema que solicita que cada clave tenga un mínimo de caracteres, combinación de letras y números, utilización de símbolos cómo #$%&, cambios periódicos e imposibilidad para tener contraseñas repetidas |
| | A9.4.4 | Uso de programas utilitarios privilegiados | No Aplica | No se cuenta con este tipo de programas |
| | A9.4.5 | Control de acceso a códigos fuente de programas | No Aplica | No se manejan códigos fuentes ni desarrollos de software. |
| **A10** | | **Criptografía** | | |
| **A10.1** | | **Controles criptográficos** | | |
| | A10.1.1 | Política sobre el uso de controles criptográficos | No Aplica | No se utilizan programas de criptografía |
| | A10.1.2 | Gestión de llaves | No Aplica | No se utilizan manejos de encriptación de llaves públicas y privadas. |

**Cuadro 1.** (Continuación)

| Declaración de aplicabilidad | | | | |
|---|---|---|---|---|
| **A11** | | **Seguridad física y del entorno** | | |
| **A11.1** | | **Áreas seguras** | | |
| | A11.1.1 | Perímetro de seguridad física | Aplica | Se cuenta con sistema de seguridad para controlar el acceso de personal no autorizado a la oficina o cuarto de sistemas. |
| | A11.1.2 | Controles de acceso físicos | Aplica | Se cuenta con sistemas de seguridad de autenticación y de control de acceso. |
| | A11.1.3 | Seguridad de oficinas, recintos e instalaciones. | Aplica | Se cuenta con sistemas de alarma para intrusos o personal no autorizado en la oficina. |
| | A11.1.4 | Protección contra amenazas externas y ambientales. | Aplica | Se cuenta con protocolos de seguridad contra eventos naturales o amenazas externas |
| | A11.1.5 | Trabajo en áreas seguras. | Aplica | Toda la infraestructura del sistema está controlado por el departamento de Talento Humano, infraestructura, tecnología y seguridad y salud en el trabajo |
| | A11.1.6 | Áreas de carga, despacho y acceso público | Aplica | No se maneja áreas de carga, despacho ni acceso al publico |
| **A11.2** | | **Equipos** | | |
| | A11.2.1 | Ubicación y protección de los equipos | Aplica | Todos los equipos se encuentra protegidos con pólizas y Backus de la información |
| | A11.2.2 | Servicios de suministro | Aplica | Los servicios suministrados externamente se realiza por medio de empresas reconocidas en el mercado por la calidad de sus productos o servicios |
| | A11.2.3 | Seguridad en el cableado. | Aplica | Todos los puntos de acceso se encuentra certificados por una empresas de seguridad |
| | A11.2.4 | Mantenimiento de los equipos. | Aplica | El mantenimiento de equipos se realiza preventivamente 1 vez semestre por una empresa especializada para dicho fin. |
| | A11.2.5 | Retiro de activos | Aplica | Los activos que son retirados de la organización por obsolescencia o daños son dispuestos para empresas que tenga manejo integral de residuos peligrosos. |
| | A11.2.6 | Seguridad de equipos y activos fuera de las instalaciones | Aplica | No se cuenta con activos por fuera de la organización |

**Cuadro 1.** (Continuación)

| Declaración de aplicabilidad | | | | |
|---|---|---|---|---|
| | A11.2.7 | Disposición segura o reutilización de equipos | Aplica | La disposición de los equipos pos consumo son entregados a entidades para el manejo de los residuos. |
| | A11.2.8 | Equipos de usuario desatendido | Aplica | Los equipos desatendidos serán diagnosticados y en los casos que haya posibilidad restablecidos para la operación. |
| | A11.2.9 | Política de escritorio limpio y pantalla limpia | Aplica | Se cuenta con un sistema de orden y aseo impulsado por el área de seguridad y salud en el trabajo. |
| **A12** | | **Seguridad de las operaciones** | | |
| **A12.1** | | **Procedimientos operacionales y responsabilidades** | | |
| | A12.1.1 | Procedimientos de operación documentados | Aplica | Todas las operaciones que se realizan dentro de la instalación se encuentran documentadas en procedimientos escritos y divulgados a todo el personal. |
| | A12.1.2 | Gestión de cambios | Aplica | Para los cambios en la organización se mantiene un procedimientos escrito |
| | A12.1.3 | Gestión de capacidad | Aplica | Se mantiene un porcentaje de capacidad del 90% para las operaciones de la organización en caso de ser necesario más se implementan nuevos activos |
| | A12.1.4 | Separación de los ambientes de desarrollo, pruebas y operación | No Aplica | No se realizan desarrollos |
| **A12.2** | | **Protección contra códigos maliciosos** | | |
| | A12.2.1 | Controles contra códigos maliciosos | Aplica | Se mantiene implementado y en funcionamiento el software de seguridad contra virus y códigos maliciosos. |
| **A12.3** | | **Copias de respaldo** | | |
| | A12.3.1 | Respaldo de la información | Aplica | Se mantiene una política de Backups de la información importante y sensible para la prestación del servicio |
| **A12.4** | | **Registro y seguimiento** | | |
| | A12.4.1 | Registro de eventos | Aplica | Se cuenta con un registro de eventos informáticos que ocurren en la organización, en la cual se analizan sus causas y se determinan controles |

**Cuadro 1.** (Continuación)

| Declaración de aplicabilidad | | | | |
|---|---|---|---|---|
| | A12.4.2 | Protección de la información de registro | Aplica | Todos los registros de la organización se encuentran guardados y asegurados en los software de calidad. |
| | A12.4.3 | Registros del administrador y del operador | Aplica | Se verifica constantemente los registros realizados por el administrador de seguridad y los parámetros de seguridad |
| | A12.4.4 | Sincronización de relojes | Aplica | Actividad automática del sistema de seguridad |
| **A12.5** | | **Control de software operacional** | | |
| | A12.5.1 | Instalación de software en sistemas operativos | Aplica | Se realiza por medio del administrador, ningún otro cargo tiene permisos suficientes para realizar instalaciones en los equipos de la organización |
| **A12.6** | | **Gestión de la vulnerabilidad técnica** | | |
| | A12.6.1 | Gestión de las vulnerabilidades técnicas | Aplica | Se mantiene un sistema de gestión del riesgo dentro de la organización |
| | A12.6.2 | Restricciones sobre la instalación de software | Aplica | Solo se instalan software que este relacionados con la prestación del servicio, la seguridad o los necesarios para la administración. |
| **A12.7** | | **Consideraciones sobre auditorias de sistemas de información** | | |
| | A12.7.1 | Controles de auditorías de sistemas de información | Aplica | Se realiza auditoria 1 vez al año por personal externo e interno para validar la seguridad de la información |
| **A13** | | **Seguridad de las comunicaciones** | | |
| **A13.1** | | **Gestión de la seguridad de las redes** | | |
| | A13.1.1 | Controles de redes | Aplica | Las redes están controladas por un LAN implementada en los puntos de red de todos los equipos. |
| | A13.1.2 | Seguridad de los servicios de red | Aplica | Las redes están protegidas tanto físicamente como digital |
| | A13.1.3 | Separación en las redes | Aplica | Solo existe un tipo de red para la prestación del servicio y la administración de la organización. |

**Cuadro 1.** (Continuación)

| Declaración de aplicabilidad | | | | |
|---|---|---|---|---|
| A13.2 | | Transferencia de información | | |
| | A13.2.1 | Políticas y procedimientos de transferencia de información | Aplica | Se implementa controles y políticas sobre la transferencia de información por medio de contratos de confidencialidad. |
| | A13.2.2 | Acuerdos sobre transferencia de información | Aplica | |
| | A13.2.3 | Mensajería Electrónica | Aplica | Se realizan auditorias periódicas para validar el contenido de los correos y su injerencia con la prestación del servicio. |
| | A13.2.4 | Acuerdos de confidencialidad o de no divulgación | Aplica | Se implementa políticas se seguridad de la información y hace parte del sistema de gestión protección de datos personales |
| **A14** | | **Adquisición, desarrollo y mantenimiento de sistemas** | | |
| **A14.1** | | **Requisitos de seguridad de los sistemas de información** | | |
| | A14.1.1 | Análisis y especificación de requisitos de seguridad de la información | Aplica | Debido al servicio que presta, la reglamentación vigente aplicable a la organización y las necesidades y expectativas de las partes interesadas se implementa un sistema de seguridad que cumpla con todas las expectativas tanto internas como externas. |
| | A14.1.2 | Seguridad de servicios de las aplicaciones en redes públicas | No Aplica | |
| | A14.1.3 | Protección de transacciones de los servicios de las aplicaciones. | No Aplica | Las transacciones realizadas por los servicios de aplicaciones están controladas por el proveedor de servicio. |
| **A14.2** | | **Seguridad en los procesos de Desarrollo y de Soporte** | | |
| | A14.2.1 | Política de desarrollo seguro | No Aplica | La organización no elabora, realiza o desarrolla ningún tipo de software para la prestación del servicio ni su comercialización. |

**Cuadro 1.** (Continuación)

| Declaración de aplicabilidad | | | | |
|---|---|---|---|---|
| | A14.2.2 | Procedimientos de control de cambios en sistemas | No Aplica | La organización no elabora, realiza o desarrolla ningún tipo de software para la prestación del servicio ni su comercialización |
| | A14.2.3 | Revisión técnica de las aplicaciones después de cambios en la plataforma de operación | No Aplica | |
| | A14.2.4 | Restricciones en los cambios a los paquetes de software | No Aplica | |
| | A14.2.5 | Principio de Construcción de los Sistemas Seguros. | No Aplica | |
| | A14.2.6 | Ambiente de desarrollo seguro | No Aplica | |
| | A14.2.7 | Desarrollo contratado externamente | No Aplica | |
| | A14.2.8 | Pruebas de seguridad de sistemas | No Aplica | |
| | A14.2.9 | Prueba de aceptación de sistemas | No Aplica | |
| **A14.3** | | **Datos de prueba** | | |
| | A14.3.1 | Protección de datos de prueba | No Aplica | No se generan datos de prueba |
| **A15** | | **Relaciones con los proveedores** | | |
| **A15.1** | | **Seguridad de la información en las relaciones con los proveedores.** | | |
| | A15.1.1 | Política de seguridad de la información para las relaciones con proveedores | Aplica | Se cuenta con una política de proveedores la cual establece los requisitos mínimos de seguridad para la prestación del servicio. |
| | A15.1.2 | Tratamiento de la seguridad dentro de los acuerdos con proveedores | Aplica | El tratamiento de seguridad se realiza conforme los contratos establecidos. |
| | A15.1.3 | Cadena de suministro de tecnología de información y comunicación | Aplica | Se cuenta con un protocolo de comunicación y una identificación plena de la cadena de suministro de información. |

**Cuadro 1.** (Continuación)

| Declaración de aplicabilidad | | | | |
|---|---|---|---|---|
| **A15.2** | | **Gestión de la prestación de servicios de proveedores** | | |
| | A15.2.1 | Seguimiento y revisión de los servicios de los proveedores | Aplica | Los servicios contratados externamente están controlados por el departamento de compras y el área de tecnología. |
| | A15.2.2 | Gestión del cambio en los servicios de los proveedores | Aplica | Los cambios en el servicio primero son validados por el departamento de tecnología y el de compras para validar su aplicabilidad en la prestación del servicio |
| **A16** | | **Gestión de incidentes de seguridad de la información** | | |
| **A16.1** | | **Gestión de incidentes y mejoras en la seguridad de la información** | | |
| | A16.1.1 | Responsabilidades y procedimientos | Aplica | La alta gerencia y el departamento de sistemas son responsables por la seguridad de la información de la organización. |
| | A16.1.2 | Reporte de eventos de seguridad de la información | Aplica | Los eventos serán documentados y analizados por el departamento de tecnología para realizar los controles necesarios. |
| | A16.1.3 | Reporte de debilidades de seguridad de la información | Aplica | Las vulnerabilidades de seguridad están identificadas, evaluadas y controladas por el departamento de seguridad como se estable en el procedimiento. |
| | A16.1.4 | Evaluación de eventos de seguridad de la información y decisiones sobre ellos | Aplica | La dirección con asesoría del departamento de seguridad implementara controles de seguridad para mitigar las causas de los eventos que se presenten. |
| | A16.1.5 | Respuesta a incidentes de seguridad de la información | Aplica | El departamento de seguridad cuenta con protocolos de actualización en caso de eventualidades para restablecer los servicios de manera que no afecte el servicio. |
| | A16.1.6 | Aprendizaje obtenido de los incidentes de seguridad de la información | Aplica | Se tiene un procedimiento de lecciones aprendidas para todos los procesos de la organización. |
| | A16.1.7 | Recolección de evidencia | Aplica | El ingeniero de sistemas por medio de un protocolo de investigación asegura la información y los activos para su estudio, investigación y análisis de los eventos que ocurran relacionados con la seguridad. |

**Cuadro 1.** (Continuación)

| Declaración de aplicabilidad | | | | |
|---|---|---|---|---|
| **A17** | | **Aspectos de seguridad de la información de la gestión de continuidad de negocio** | | |
| **A17.1** | | **Continuidad de Seguridad de la información** | | |
| | A17.1.1 | Planificación de la continuidad de la seguridad de la información | Aplica | Se cuenta con un plan de continuidad del negocio donde se establece la manera de actuar al momento de un evento que afecte la información o los activo. |
| | A17.1.2 | Implementación de la continuidad de la seguridad de la información | Aplica | Dentro del plan de continuidad del negocio se establecen las medidas para la seguridad de la información después de un evento que afecte la información o los activos |
| | A17.1.3 | Verificación, revisión y evaluación de la continuidad de la seguridad de la información | Aplica | Se cuenta con las herramientas necesarias para validar el sistema de seguridad implementado. |
| **A17.2** | | **Redundancias** | | |
| | A17.2.1 | Disponibilidad de instalaciones de procesamiento de información | No Aplica | No se cuenta con otras instalaciones |
| **A18** | | **Cumplimiento** | | |
| **A18.1** | | **Cumplimiento de requisitos legales y contractuales** | | |
| | A18.1.1 | Identificación de la legislación aplicable. | Aplica | Se tiene identificado plenamente los requisitos de ley aplicables a la organización, el servicio prestado y las características propias de la información. |
| | A18.1.2 | Derechos propiedad intelectual (DPI) | No aplica | No se cuenta con desarrollos o información que puede ser catalogado como de propiedad intelectual. |
| | A18.1.3 | Protección de registros | Aplica | Los registros del servicio prestado se encuentra protegidos tanto física como digitalmente. |
| | A18.1.4 | Privacidad y protección de información de datos personales | Aplica | Se tiene implementado un sistema de protección de datos personales |
| | A18.1.5 | Reglamentación de controles criptográficos. | No Aplica | No se cuenta con herramientas ni protocolos de encriptación ni criptografía. |

**Cuadro 1.** (Continuación)

| Declaración de aplicabilidad | | | | |
|---|---|---|---|---|
| **A18.2** | | **Revisiones de seguridad de la información** | | |
| | A18.2.1 | Revisión independiente de la seguridad de la información | Aplica | Se realiza revisión por la dirección una vez al año para validar los eventos que han afectado a la seguridad, validando el cumplimiento de políticas y normas de seguridad así como la revisión técnica que se realiza. |
| | A18.2.2 | Cumplimiento con las políticas y normas de seguridad | Aplica | |
| | A18.2.3 | Revisión del cumplimiento técnico | Aplica | |

**Fuente:** Propia

Con la declaración de aplicabilidad realizada se establece las vulnerabilidades y riesgos que posee la organización relacionada a la seguridad, esta información es base para la implementación de un SGSI enfocado en disminuir, eliminar, trasferir o controlar los factores causantes del riesgo.

### 4.1.3 Situación de la organización

La aplicación de la declaración de aplicabilidad en la Move Cargo S.A. muestra que tiene implementado sistemas informáticos y controles para la planificación y mantenimiento y mejorar de un SGSI al interior de la organización.

Del total de los controles especificados por la norma ISO 27001 Move Cargo S.A. cumple con un 61.67% de los 114 requisitos mencionados como se detalla en el cuadro 2.

**Cuadro 2.** Situación de la empresa

| Requisitos y controles | | No de requisitos | Aplicabilidad |
|---|---|---|---|
| **A5** | **Políticas de la seguridad de la información** | **2** | **100 %** |
| **A6** | **Organización de la seguridad de la información** | **7** | **71.4 %** |
| **A7** | **Seguridad de los recursos humanos** | **6** | **100 %** |
| **A8** | **Gestión de activos** | **10** | **90 %** |
| **A9** | **Control de acceso** | **14** | **85.7 %** |

Cuadro 2. (Continuación)

| Requisitos y controles | | No de requisitos | Aplicabilidad |
|---|---|---|---|
| **A10** | **Criptografía** | **2** | **0 %** |
| **A11** | **Seguridad física y del entorno** | **15** | **100 %** |
| **A12** | **Seguridad de las operaciones** | **14** | **92.8 %** |
| **A13** | **Seguridad de las comunicaciones** | **7** | **100 %** |
| **A14** | **Adquisición, desarrollo y mantenimiento de sistemas** | **13** | **7.69 %** |
| **A15** | **Relaciones Con Los Proveedores** | **5** | **100 %** |
| **A16** | **Gestión de incidentes de seguridad de la información** | **7** | **100 %** |
| **A17** | **Aspectos de seguridad de la información de la gestión de continuidad de negocio** | **4** | **75 %** |
| **A18** | **Cumplimiento** | **8** | **87.5 %** |
| **Total** | | **114** | **61.67 %** |

Para los aspectos que no son aplicables debido a la naturaleza del negocio o a la metodología utilizada para la implementación del sistema informático se tomaran acciones y controles específicos.

Con la aplicación de la declaración de aplicabilidad en Move cargo se pudo establecer cuáles son los puntos críticos a tener en cuenta para la implementación del SGSI, como lo es él envió de información importante de manera criptográfica y la adquisición, desarrollo y mantenimiento de sistemas.

## 4.2 ANÁLISIS Y EVALUACIÓN DE RIESGOS Y VULNERABILIDADES

Se utilizó la metodología MAGERIT la cual es un modelo de análisis y gestión de riesgos a sistemas informáticos adaptable a cualquier tipo y tamaño de organización.

Para realizar la valoración de riesgos se identificaron los activos informáticos de la organización los cuales están divididos en subgrupos como se mostró en el numeral 4.1.1.

- D - Datos informáticos:
- SW - Software:
- HW Hardware:
- Media soporte de información
- Aux equipamiento auxiliar
- COM - redes de comunicaciones
- P – Personal

Para poder determinar la importancia de cada uno de los activos identificados por la organización se califican las dimensiones del cuadro 3.

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión. Para la valoración de los activos se utilizan los criterios que se muestran en el cuadro 4.

**Cuadro 3.** Valoración de dimensiones

| Valor | *Dimensiones* |
|---|---|
| D | Disponibilidad |
| I | Integridad de los datos |
| C | Confidencialidad de los datos |
| A | Autenticidad de los usuarios y de la información |
| T | Trazabilidad del servicio y de los datos |

Cuadro 4. **Valoración de activos**

| *Valor* | *Criterio* |
|---|---|
| 10 | Daño muy grave a la organización |
| 7-9 | Daño grave a la organización |
| 4-6 | Daño importante a la organización |
| 1-3 | Daño menor a la organización |
| 0 | Irrelevante para la organización |

### 4.2.1 Valoración de activos informativos

Cuadro 5. **Valoración de activos**

| Clasificación | Activo | Dimensiones | | | | | Total |
|---|---|---|---|---|---|---|---|
| | | D | I | C | A | T | |
| [D] DATOS/INFORMACIÓN | Base de datos de declaraciones presentadas | 10 | 10 | 10 | 10 | 10 | 50 |
| | Clasificación arancelaria por producto | 10 | 10 | 10 | 10 | 10 | 50 |
| [SW] SOFTWARE | Software contable - Informa web | 10 | 10 | 9 | 10 | 10 | 49 |
| | Software operativo - SIACOMEX, VUCE, ALAS, PREIMPO | 10 | 10 | 10 | 8 | 10 | 48 |
| | Software de gestión – Daruma | 8 | 8 | - | 10 | 9 | 35 |
| | Microsoft Windows 7 | 8 | - | - | 10 | 9 | 27 |
| | Antivirus | - | - | - | - | 9 | 9 |
| | Ofimática | - | - | - | - | 7 | 7 |
| [HW] HARDWARE | 60 Computadores Fijos bajo la modalidad de arrendamiento. | 9 | - | - | - | 8 | 17 |
| | Servidor ZEUS | 10 | - | - | - | 10 | 20 |
| | Servidor HÉRCULES | 9 | - | - | - | 9 | 18 |
| | Servidor LINUX | 8 | - | - | - | 9 | 17 |
| | Servidor MTS | 9 | - | - | - | 9 | 18 |
| | Servidor BOEING | 9 | - | - | - | 9 | 18 |
| | Servidor SENECA | 9 | - | - | - | 9 | 18 |
| | UTM Fortinet | 10 | - | - | - | 9 | 19 |
| | Impresora A – B | 8 | - | - | - | 9 | 17 |

Cuadro 5. (Continuación)

| Clasificación | Activo | Dimensiones | | | | | Total |
|---|---|---|---|---|---|---|---|
| | | D | I | C | A | T | |
| [MS] MEDIA SOPORTE DE INFORMACIÓN | Discos de información extraíbles | 7 | - | - | - | - | 7 |
| | CD | 6 | - | - | - | - | 6 |
| [AUX] EQUIPAMIENTO AUXILIAR | Planta eléctrica del edificio | 9 | - | - | - | - | 9 |
| | UPS | 10 | - | - | - | - | 10 |
| | Aire acondicionado | 7 | - | - | - | - | 7 |
| | Infraestructura eléctrica | 10 | - | - | - | - | 10 |
| [COM] REDES DE COMUNICACIONES | Redes de teléfono | 9 | - | - | - | - | 9 |
| | Correos electrónicos | 8 | - | - | - | - | 8 |
| | Red WIFI | 9 | - | - | - | - | 9 |
| | Internet | 9 | - | - | - | - | 9 |
| [P] PERSONAL | Ingeniero de sistemas | 8 | - | 9 | - | - | 17 |
| | Ingeniero de desarrollo | 8 | - | 9 | - | - | 17 |
| | Coordinador de Infraestructura, Tecnología y SIG | 8 | - | 9 | - | - | 17 |

### 4.2.2 Identificación de riesgos, vulnerabilidades y amenazas

Como parte del análisis se identificaron las posibles amenazas y riesgos que pueden afectar a la información, activos o infraestructura de la organización y por ende afectar la prestación del servicio.

[N] Desastres naturales
[N.1] Fenómeno Climático
[N.2] Fenómeno Sísmico
[N.3] Fenómeno de origen volcánico
[N.4] Fenómeno meteorológico
[N.5] Inundación

[I] Desastres industriales
[I.1] Fuego
[I.2] Daños por agua
[I.3] Explosiones
[I.4] Sobrecarga eléctrica
[I.5] Contaminación mecánica (Polvo, vibración, suciedad, etc.)
[I.6] Avería de origen físico o lógico
[I.7] Corte de suministro eléctrico
[I.8] Condiciones inadecuadas de temperatura o humedad
[I.9] Fallo de servicio de comunicación (Internet, Teléfono. Etc.)
[I.10] Interrupción de servicios esenciales
[I.11] Degradación de soportes de almacenamiento de la información

[E] Errores y fallos no intencionados
[E.1] Errores de usuario
[E.2] Errores de administrador
[E.3] Errores de monitorización
[E.4] Errores de configuración
[E.5] Difusión de software dañino
[E.6] Escapes de información
[E.7] Alteración accidental de la información
[E.8] Destrucción de la información
[E.9] Fugas de información
[E.10] Vulnerabilidades de los programas (software)
[E.11] Errores de mantenimiento / actualización de programas (software)
[E.12] Errores de mantenimiento / actualización de equipos (hardware)
[E.13] Perdida de equipos
[E.14] Indisponibilidad del personal

[A] Ataques intencionados
[A.1] Manipulación de los registros de actividad

[A.2] Manipulación de la configuración
[A.3] Suplantación de la identidad del usuario
[A.4] Abuso de privilegios de acceso
[A.5] Difusión de software dañino (malware)
[A.6] Re encaminamiento de mensajes
[A.7] Alteración de secuencia
[A.8] Acceso no autorizado
[A.9] Modificación deliberada de información
[A.10] Destrucción de información
[A.11] Divulgación de información
[A.12] Manipulación malintencionada de programas
[A.13] Manipulación malintencionada de equipos
[A.14] Robo
[A.15] Ataque destructivo
[A.16] Ingeniería social

### 4.2.3 Valoración de amenazas

Para la valoración de las amenazas se tiene en cuenta el grado de afectación (el cuadro 6) y las dimensiones de los activos que son afectadas (cuadro 7).

**Cuadro 6.** Valoración de amenazas

| Calificación | | Explicación |
|---|---|---|
| A | *1* | *Se afecta en un 100% hasta un 76 %* |
| M+ | *0.75* | *Se afecta en un 75% hasta un 51 %* |
| M | *0.5* | *Se afecta en un 50% hasta un 26 %* |
| M- | *0.25* | *Se afecta en un 25% hasta un 11 %* |
| B | *0.1* | *Se afecta en un 10% o menos* |

**Cuadro 7.** Valoración de activos

| Calificación | Explicación | Abr. |
|---|---|---|
| Degradación de la confidencialidad | Grado en el cual el activo pierde confidencialidad o es publicado. | DC |
| Degradación de integridad | Grado en el que se pierde, modifica o se manipula la información. | DI |
| Degradación de disponibilidad | Grado en el que se pierde el acceso de la información. | DD |
| Degradación de la autenticidad | Grado de deterioro en el cual no se puede constatar la autenticidad de la información. | DA |
| Degradación de la trazabilidad | Grado en el cual no se puede realizar seguimiento a la fuente de información. | DT |

Cuadro 8. **Identificación de amenazas**

| Activo | Riesgos | DC | DI | DD | DA | DT |
|---|---|---|---|---|---|---|
| D DATOS/INFORMACIÓN<br><br>Base de datos de declaraciones presentadas<br>Clasificación arancelaria por producto | [N] Desastres naturales<br><br>Fenómeno Climático<br>Fenómeno Sísmico<br>Fenómeno de Origen Volcánico<br>Fenómeno de origen Meteorológico<br>Inundaciones | M | M+ | A | M+ | M+ |
| | [I] Desastres industriales<br><br>Fuego<br>Daños por agua<br>Desastres Industriales<br>Contaminación mecánica<br>Contaminación electromagnética<br>Averías de Origen físico o lógico<br>Condiciones inadecuadas de temperatura o humedad<br>Degradación de los soportes de almacenamiento de la información | M | M+ | M+ | M | M+ |
| | [E] Errores y fallos no intencionados<br><br>Errores de usuario<br>Errores de administrador<br>Errores de configuración | M | M- | M- | M | M |

**Cuadro 8.** (Continuación)

| Activo | Riesgos | DC | DI | DD | DA | DT |
|---|---|---|---|---|---|---|
| D DATOS/INFORMACIÓN<br><br>Base de datos de declaraciones presentadas<br>Clasificación arancelaria por producto | [A] Ataques malintencionados<br><br>Manipulación de los registros de actividades<br>Manipulación de la configuración<br>Suplantación de la identidad del usuario<br>Difusión de software dañino<br>Acceso no autorizado<br>Destrucción de la información<br>Robo<br>Ataque destructivo<br>Ingeniería social | M+ | M+ | M | M+ | M- |
| SW SOFTWARE<br><br>Software contable - Informa web<br>Software operativo - SIACOMEX, VUCE, ALAS, PREIMPO<br>Software de gestión – Daruma<br>Microsoft Windows 7<br>Antivirus<br>Ofimática | [N] Desastres naturales<br><br>Fenómeno Climático<br>Fenómeno Sísmico<br>Fenómeno de Origen Volcánico<br>Fenómeno de origen Meteorológico<br>Inundaciones | M | M+ | M+ | M | M+ |

**Cuadro 8.** (Continuación)

| Activo | Riesgos | DC | DI | DD | DA | DT |
|---|---|---|---|---|---|---|
| SW SOFTWARE<br><br>Software contable - Informa web<br>Software operativo - SIACOMEX, VUCE, ALAS, PREIMPO<br>Software de gestión – Daruma<br>Microsoft Windows 7<br>Antivirus<br>Ofimática | [I] Desastres industriales<br><br>Fuego<br>Daños por agua<br>Averías de Origen físico o lógico<br>Condiciones inadecuadas de temperatura o humedad<br>Degradación de los soportes de almacenamiento de la información<br>Eliminación electromagnética | M- | M+ | M+ | M- | M+ |
| | [E] Errores y fallos no intencionados<br><br>Errores de usuario<br>Errores de administrador<br>Errores de configuración<br>Deficiencias de la organización<br>Errores de mantenimiento / actualización de programas de software<br>Perdida de equipos<br>Indisponibilidad del personal | M- | M+ | M | M- | M- |

**Cuadro 8.** (Continuación)

| Activo | Riesgos | DC | DI | DD | DA | DT |
|---|---|---|---|---|---|---|
| SW SOFTWARE<br><br>Software Contable - Informa web<br>Software operativo - Customsgm, VUCE, ALAS, PREIMPO<br>Software de gestión – Daruma<br>Microsoft Windows 7<br>Antivirus<br>Ofimática | [A] Ataques Intencionados<br><br>Manipulación de los registros de actividades<br>Manipulación de la configuración<br>Suplantación de la identidad del usuario<br>Abuso de privilegios de acceso<br>Modificación deliberada de la información<br>Difusión de software dañino<br>Acceso no autorizado<br>Destrucción de la información<br>Robo<br>Ataque destructivo<br>Manipulación de programas<br>Manipulación de los equipos<br>Ingeniería social | M- | M+ | M+ | M | M- |

**Cuadro 8.** (Continuación)

| Activo | Riesgos | DC | DI | DD | DA | DT |
|---|---|---|---|---|---|---|
| HW HARDWARE<br><br>60 Computadores Fijos bajo la modalidad de arrendamiento.<br>Servidor ZEUS<br>Servidor HÉRCULES<br>Servidor LINUX<br>Servidor MTS<br>Servidor BOEING<br>Servidor SENECA<br>UTM Fortinet<br>Impresora A – B | [N] Desastres naturales<br><br>Fenómeno Climático<br>Fenómeno Sísmico<br>Fenómeno de Origen Volcánico<br>Fenómeno de origen Meteorológico<br>Inundaciones | M | M | A | M | M+ |
| | [I] Desastres industriales<br><br>Fuego<br>Daños por agua<br>Averías de Origen físico o lógico<br>Condiciones inadecuadas de temperatura o humedad<br>Eliminación electromagnética<br>Interrupción de otros servicios y suministros esenciales<br>Emanaciones electromagnéticas | B | M- | M+ | M | M- |

**Cuadro 8.** (Continuación)

| Activo | Riesgos | DC | DI | DD | DA | DT |
|---|---|---|---|---|---|---|
| HW HARDWARE<br><br>60 Computadores Fijos bajo la modalidad de arrendamiento.<br>Servidor ZEUS<br>Servidor HÉRCULES<br>Servidor LINUX<br>Servidor MTS<br>Servidor BOEING<br>Servidor SENECA<br>UTM Fortinet<br>Impresora A – B | [E] Errores y fallos no intencionados<br><br>Errores de usuario<br>Errores de administrador<br>Errores de configuración<br>Deficiencias de la organización<br>Errores de mantenimiento / actualización de programas de software<br>Perdida de equipos<br>Indisponibilidad del personal | M+ | M | M+ | M- | M |
| | [A] Ataques Intencionados<br><br>Manipulación de la configuración de seguridad<br>Difusión de software dañino<br>Abuso de privilegios de acceso<br>Acceso no autorizado<br>Robo<br>Ataque destructivo<br>Manipulación de los equipos | M- | M- | M+ | M | M- |

**Cuadro 8.** (Continuación)

| Activo | Riesgos | DC | DI | DD | DA | DT |
|---|---|---|---|---|---|---|
| SOPORTE DE INFORMACIÓN<br><br>Discos de información extraíbles<br>CD | [N] Desastres naturales<br><br>Fenómeno Climático<br>Fenómeno Sísmico<br>Fenómeno de Origen Volcánico<br>Fenómeno de origen Meteorológico<br>Inundaciones | M | M- | M+ | M- | M+ |
| | [I] Desastres industriales<br><br>Fuego<br>Daños por agua<br>Averías de Origen físico o lógico<br>Condiciones inadecuadas de temperatura o humedad<br>Eliminación electromagnética | B | B | M- | B | B |
| | [E] Errores y fallos no intencionados<br><br>Errores de usuario<br>Errores de configuración<br>Errores de mantenimiento<br>Perdida de equipos<br>Indisponibilidad del personal | M | M | M- | M | M- |

**Cuadro 8.** (Continuación)

| Activo | Riesgos | DC | DI | DD | DA | DT |
|---|---|---|---|---|---|---|
| SOPORTE DE INFORMACIÓN<br><br>Discos de información extraíbles<br>CD | [A] Ataques Intencionados<br><br>Difusión de software dañino<br>Abuso de privilegios de acceso<br>Acceso no autorizado<br>Robo<br>Ataque destructivo | M | M | M- | M- | M+ |
| AUX EQUIPAMIENTO AUXILIAR<br><br>Planta eléctrica del edificio<br>UPS<br>Aire acondicionado<br>Infraestructura eléctrica | [N] Desastres naturales<br><br>Fenómeno Climático<br>Fenómeno Sísmico<br>Fenómeno de Origen Volcánico<br>Fenómeno de origen Meteorológico<br>Inundaciones | M | M- | M+ | M- | M+ |
| | [I] Desastres industriales<br><br>Fuego<br>Daños por agua<br>Desastres industriales<br>Averías de Origen físico o lógico<br>Condiciones inadecuadas de temperatura o humedad | M- | M | M+ | M- | M |

**Cuadro 8.** (Continuación)

| Activo | Riesgos | DC | DI | DD | DA | DT |
|---|---|---|---|---|---|---|
| AUX EQUIPAMIENTO AUXILIAR<br><br>Planta eléctrica del edificio<br>UPS<br>Aire acondicionado<br>Infraestructura eléctrica | [E] Errores y fallos no intencionados<br><br>Errores de usuario<br>Errores de administración<br>Errores de mantenimiento<br>Perdida de equipos | M- | M- | M+ | M- | M |
| | [A] Ataques Intencionados<br><br>Abuso de privilegios de acceso<br>Acceso no autorizado<br>Robo<br>Ataque destructivo | M- | M- | M+ | M- | M- |
| COM REDES DE COMUNICACIONES<br><br>Redes de teléfono<br>Correos electrónicos<br>Red WIFI<br>Internet | [N] Desastres naturales<br><br>Fenómeno Climático<br>Fenómeno Sísmico<br>Fenómeno de Origen Volcánico<br>Fenómeno de origen Meteorológico<br>Inundaciones | M | M+ | M+ | M- | M+ |

**Cuadro 8.** (Continuación)

| Activo | Riesgos | DC | DI | DD | DA | DT |
|---|---|---|---|---|---|---|
| COM REDES DE COMUNICACIONES<br><br>Redes de teléfono<br>Correos electrónicos<br>Red WIFI<br>Internet | [I] Desastres industriales<br><br>Fuego<br>Daños por agua<br>Desastres industriales<br>Averías de Origen físico o lógico<br>Condiciones inadecuadas de temperatura o humedad<br>Fallo de servicio esenciales<br>Degradación de los soportes de almacenamiento de la información | M- | M- | M+ | M | M- |
| | [E] Errores y fallos no intencionados<br><br>Errores de usuario<br>Errores de administración<br>Errores de configuración<br>Difusión de software maligno<br>Alteración no intencionada de información<br>Errores de mantenimiento<br>Perdida de equipos<br>Caída de sistemas por agotamiento de recursos | M- | M- | M | M- | M+ |

**Cuadro 8.** (Continuación)

| Activo | Riesgos | DC | DI | DD | DA | DT |
|---|---|---|---|---|---|---|
| COM REDES DE COMUNICACIONES<br><br>Redes de teléfono<br>Correos electrónicos<br>Red WIFI<br>Internet | [A] Ataques Intencionados<br><br>Manipulación de la configuración<br>Suplantación de la identidad del usuario<br>Abuso de privilegios de acceso<br>Acceso no autorizado<br>Difusión de software dañino<br>Manipulación de programas<br>Robo<br>Denegación del servicio<br>Ataque destructivo | M- | M- | M+ | M | M- |
| P PERSONAL<br><br>Ingeniero de sistemas<br>Ingeniero de desarrollo<br>Coordinador de Infraestructura, Tecnología y SIG | [N] Desastres naturales<br><br>Fenómeno Climático<br>Fenómeno Sísmico<br>Fenómeno de Origen Volcánico<br>Fenómeno de origen Meteorológico<br>Inundaciones | M | M | M+ | M | M+ |
| | [I] Desastres industriales<br><br>Fuego<br>Desastres industriales<br>Condiciones inadecuadas de temperatura o humedad | M- | M- | M+ | M | M+ |

**Cuadro 8.** (Continuación)

| Activo | Riesgos | DC | DI | DD | DA | DT |
|---|---|---|---|---|---|---|
| P PERSONAL<br><br>Ingeniero de sistemas<br>Ingeniero de desarrollo<br>Coordinador de Infraestructura, Tecnología y SIG | [E] Errores y fallos no intencionados<br>Errores de usuario<br>Errores de administración<br>Errores de configuración<br>Difusión de software maligno<br>Alteración no intencionada de información<br>Errores de mantenimiento<br>Perdida de equipos<br>Fugas de información<br>Errores de actualización<br>Indisponibilidad del personal | M+ | M+ | M- | M+ | M |
| | [A] Ataques Intencionados<br>Manipulación de registro de actividad<br>Manipulación de la configuración<br>Suplantación de la identidad del usuario<br>Uso no previsto<br>Re encaminamiento de mensajes<br>Abuso de privilegios de acceso<br>Modificación deliberada de información<br>Acceso no autorizado<br>Difusión de software dañino<br>Manipulación de programas<br>Robo<br>Denegación del servicio<br>Ataque destructivo | A | A | M+ | M | M- |

### 4.2.4 Evaluación de vulnerabilidades, amenazas y riesgos.

Como mecanismo para evaluar los riesgos y vulnerabilidades que se presentan en la Move Cargo S.A. Se identifican los impactos de la materialización de riesgo contra la probabilidad de ocurrencia del riesgo.

**Cuadro 9.** Identificación de riesgo

| No | Riesgo o vulnerabilidad | Riegos potenciales |
|---|---|---|
| HARDWARE | | |
| R1 | Pérdida o daños en la infraestructura por eventos naturales. | Perdida de información sensible, valiosa y necesaria para prestar el servicio de agenciamiento aduanero. |
| R2 | Alteraciones del entorno de los sistemas de almacenamiento. | Daños en la infraestructura de sistema operativo, lo que originaría vulnerabilidades, perdidas de información o deterioro. |
| R3 | Acceso abusivo a los sistemas informáticos y operativos de la organización | Posibles robos, alteraciones, eliminación o fugas de información sensible o confidencial de la organización. |
| | | Daños en los sistemas operativos, de almacenamiento o de seguridad implementados por la organización. |
| R4 | Fallas de equipos por cortes de energía o sobre carga en los equipos | Perdida de la información, daños en los equipos y retrasos en la operación normal. |
| R5 | Daños intencionales a la infraestructura de la organización | Perdida de información y vulnerabilidad en los sistema de seguridad. |
| R6 | Hurto de hardware o activos de la infraestructura informática | Perdida de la capacidad para procesar información, proteger el sistema o prestar el servicio |
| R7 | Manipulación de equipos sin controles | Daños o pérdida de funcionalidad de los equipos |

**Cuadro 9.** (Continuación)

| No | Riesgo o vulnerabilidad | Riegos potenciales |
|---|---|---|
| HARDWARE | | |
| R8 | Cuarto de sistemas sin medidas de seguridad | Robo o daños en los equipos de cómputo, servidores, telecomunicación o elementos para el almacenamiento de la información |
| R9 | Control de acceso físico a las oficinas inexistentes o deficientes | |
| SOFTWARE | | |
| R10 | Propagación de virus o malware en los equipos de la organización | Daños en el software y sistemas operativos necesarios para la prestación del servicio. |
| R11 | Software no licenciados | Mal funcionamiento del software operativo, fallas en la prestación del servicio |
| R12 | Desarrollo propios con fallas de seguridad | Posibles ataques externos ocasionando fallas en el funcionamiento del software, perdida de información o fallas en la prestación del servicio. |
| R13 | Sistemas operativos obsoletos | Posibles accesos de virus y fallas en los sistemas de seguridad |
| R14 | Falta de control en las Instalaciones de software en los sistemas informáticas | Fallas en los software de la organización, propagación de virus o pérdidas de la información. |
| SOPORTE DE INFORMACIÓN | | |
| R15 | Daños en los soportes de la información | Perdida de los Backups o información del servicio |
| R16 | Perdida de los soportes de la información | Posibles fugas de información sensible o importante para la organización. |
| EQUIPAMIENTO AUXILIAR | | |
| R17 | Fallas eléctricas o daños en la infraestructura eléctrica | Daños los equipos auxiliares UPS, aire acondicionado, estructura eléctrica |

**Cuadro 9.** (Continuación)

| No | Riesgo o vulnerabilidad | Riegos potenciales |
|---|---|---|
| REDES DE COMUNICACIONES | | |
| R18 | Fallas en el suministro del servicio de comunicación (Internet, teléfono, correo) | Demoras en la prestación del servicio y fallas de comunicación |
| R19 | Intercepción de comunicación sensible o confidencial por medios magnéticos | Utilización de herramientas para interceptar comunicaciones |
| R20 | Fallas en la planta telefónica, redes de internet o red WIFI | Demoras en los proceso y prestación del servicio, fallas de comunicación y posible pérdida de información |
| R21 | Suplantación del sitio web de la organización | Fallas en los sistemas de comunicación internos y externos |
| PERSONAL | | |
| R22 | Personal con pocos conocimientos en informática o sistemas de seguridad | Posibles vulnerabilidades para el ingreso de virus o ransomware que afecten al sistema de seguridad. |
| R23 | Fallas involuntarias en la implementación o configuración de los sistemas de seguridad | Vulnerabilidades que puede ser aprovechada para el robo, manipulación o modificación de la información de la organización. |
| R24 | Trasferencia no consentida de activos empresariales | Perdida de confidencialidad de la información y posibles sanciones legales o económicas por los clientes |
| R25 | Modificación, eliminación o publicación de información sensible de la organización sin previa autorización. | Perdida de información, afectación para la prestación del servicio y perdida de la integridad de la información |
| R26 | Soporte técnico deficiente para resolver problemas internos | Falta de sistemas informático eficiente y confiable para la prestación del servicio. |
| R27 | Modificación mal intencionada de los parámetros de seguridad establecidos (Backus, firewall, antivirus, Etc.) | Vulnerabilidad en los sistemas de seguridad |

### 4.2.5 Valoración de vulnerabilidad y nivel de riesgo

Como parte del análisis se identificaron las posibles amenazas y riesgos que pueden afectar a la información, activos o infraestructura de la organización y por ende afectar la prestación del servicio.

Para poder determinar el valor de los riesgos identificados contra los activos de la organización se determinar un escenario en el que se verifica la probabilidad de ocurrencia de los riesgos contra los impactos generados en los sistemas de seguridad, información o activos de la organización.

Los riesgos son medidos por medio de matrices de probabilidad y de impactos descritas a continuación.

**Probabilidad de ocurrencia**

Es la probabilidad que tiene un evento de ocurrir bajo una serie de circunstancias y parámetros. Esta se califica por la cantidad de veces que puede ocurrir dentro de un rango de tiempo determinado.

**Cuadro 10.** Probabilidad de ocurrencia

| Calificación | Descripción | Rango |
|---|---|---|
| Casi imposible | *Es remota la posibilidad de que el evento ocurra incluso bajo circunstancias favorables.* | *1 vez al año o nunca* |
| Improbable | *Es posible que el evento ocurra solo cuando se presente condiciones favorables, estas condiciones son anormales y a típicas.* | *1 vez cada semestre* |
| Posible | *Se puede suponer que el evento ocurra bajo circunstancias normales* | *1 vez cada 2 meses* |
| Probable | *Se espera que el evento ocurra bajo cualquier circunstancia posible* | *1 vez por semana* |
| Casi seguro | *El evento tiene altas posibilidades de ocurrir bajo cualquier circunstancia.* | *1 vez por día* |

**Impacto generado**
Es la relación de daños que se obtiene de la materialización del riesgo dentro de la organización los cuales afecten a los activos de la organización, el impacto se mide por el % de afectación de los activos o su daño en la información.

**Cuadro 11.** Impactos

| Impacto | Descripción | Rango |
|---|---|---|
| Mínimo | Afección mínima a los activos. Fácilmente recuperables. | Entre 0% y 10% |
| Medio | Afección media a los activos. Posibles alteraciones de la información o activos. | Entre 11% y 25% |
| Moderado | Afección moderada a los activos. Posibles pérdidas de información o funcionalidad de los activos. | Entre 26% y 50% |
| Alto | Afección alta a los activos. Eliminaciones, modificación, alteración o fallas en la funcionalidad de los activos, difícil de recuperar. | Entre 51% y 75% |
| Catastrófico | Afección alta a los activos. Eliminaciones, modificación, alteración o fallas en la funcionalidad de los activos, Imposible recuperar | Entre 76% y 100% |

Para valorar el nivel de riesgo que tiene los activos de información se realiza la valoración con base en la información del cuadro 12.

**Cuadro 12.** Cuadro de valoración

| Calificación | Explicación | Abr. |
|---|---|---|
| Riesgo Catastrófico | Los impactos de las amenazas a la información seria irrecuperables | RC |
| Riesgo Alto | Los impactos de las amenazas a la información seria considerables | RA |
| Riesgo Medio | Los impactos de las amenazas a la información seria moderados y recuperables | RM |
| Riesgo Bajo | Los impactos de las amenazas a la información seria mínimos | RB |
| Riesgo Aceptable | Los impactos de las amenazas a la información no sería mismos y seria fáciles de recuperar | RAC |

La valoración de cada riesgo y vulnerabilidad se realiza conforme la probabilidad de ocurrencia y su impacto en la organización, como se especifica en el cuadro 13.

**Cuadro 13.** Cuadro de evaluación

| Evaluación de riesgos | | | | | |
|---|---|---|---|---|---|
| Probabilidad de ocurrencia | Mínimo | Medio | Moderado | Alto | Catastrófico |
| Casi imposible | RAC | RAC | RB | RB | RM |
| Improbable | RAC | RB | RM | RM | RM |
| Posible | RB | RM | RM | RA | RA |
| Probable | RB | RM | RA | RA | RC |
| Casi seguro | RM | RM | RA | RC | RC |

Con los parámetros determinados se realiza valoración de riesgos y vulnerabilidad y los resultados se muestran en el cuadro 14.

**Cuadro 14.** Evaluación del riesgo y vulnerabilidad

| Identificación | | | Evaluación | | |
|---|---|---|---|---|---|
| Riesgo | Activo | Consecuencia | Probabilidad | Impacto esperado | Nivel de riesgo |
| R1. Pérdida o daños en la infraestructura por eventos naturales. | HARDWARE | Imposibilidad para la prestación del servicio | Improbable | Alto | RM |
| R2. Alteraciones del entorno de los sistemas de almacenamiento. | | Perdidas de información | Improbable | Alto | RM |
| R3. Acceso abusivo a los sistemas informáticos y operativos de la organización | | Alteración de la información | Posible | Moderado | RM |
| R4. Fallas de equipos por cortes de energía o sobre carga en los equipos | | Falla en los equipos | Improbable | Medio | RAC |
| R5. Daños intencionales a la infraestructura de la organización | | Perdida de información | Improbable | Moderado | RB |
| R6. Hurto de hardware o activos de la infraestructura informática | | Retrasos en la prestación del servicio | Posible | Alto | RA |
| R7. Manipulación de equipos sin controles | | Perdida de seguridad | Improbable | Moderado | RB |
| R8. Cuarto de sistemas sin medidas de seguridad | | Robo o hurto de activos | Posible | Catastrófico | RC |
| R9. Control de acceso físico a las oficinas inexistentes o deficientes | | Pérdidas materiales del sistema de seguridad | Posible | Catastrófico | RC |

**Cuadro 14.** (Continuación)

| Identificación | | | Evaluación | | |
|---|---|---|---|---|---|
| Riesgo | Activo | Consecuencia | Probabilidad | Impacto esperado | Nivel de riesgo |
| R10. Propagación de virus o malware en los equipos de la organización | SOFTWARE | Fallas en los sistemas | Posible | Alto | RA |
| R11. Software no licenciados | | Posible pérdida de información | Improbable | Mínimo | RAC |
| R12. Desarrollo propios con fallas de seguridad | | Acceso a información | Improbable | Medio | RAC |
| R13. Sistemas operativos obsoletos | | Fallas en seguridad | Improbable | Medio | RAC |
| R14. Falta de control en las Instalaciones de software en los sistemas informáticos | | Propagación de virus | Posible | Alto | RA |

**Cuadro 14.** (Continuación)

| Identificación | | | Evaluación | | |
|---|---|---|---|---|---|
| Riesgo | Activo | Consecuencia | Probabilidad | Impacto esperado | Nivel de riesgo |
| R15. Daños en los soportes de la información | SOPORTE DE INFORMACIÓN | Perdida de información | Posible | Alto | RA |
| R16. Perdida de los soportes de la información | | Falta de herramientas para guardar información | Improbable | Alto | RM |
| R17. Fallas eléctricas o daños en la infraestructura eléctrica | AUX EQUIPAMIENTO | Daños en los activos | Posible | Catastrófico | RC |
| R18. Fallas en el suministro del servicio de comunicación (Internet, teléfono, correo) | REDES DE COMUNICACIONES | Perdida de la capacidad para suministrar el servicio | Improbable | Alto | RM |
| R19. Intercepción de comunicación sensible o confidencial por medios magnéticos | | Pérdida de credibilidad | Posible | Alto | RA |

**Cuadro 14.** (Continuación)

| Identificación | | | Evaluación | | |
|---|---|---|---|---|---|
| Riesgo | Activo | Consecuencia | Probabilidad | Impacto esperado | Nivel de riesgo |
| R20. Fallas en la planta telefónica, redes de internet o red WIFI | REDES DE COMUNICACIONES | Retrasos en la operación y pérdida de capacidad | Posible | Alto | RA |
| R21. Suplantación del sitio web de la organización | | Suplantación de la empresa | Posible | Moderado | RM |
| R22. Personal con pocos conocimientos en informática o sistemas de seguridad | PERSONAL | Posibles abertura de seguridad | Posible | Mínimo | RB |
| R23. Fallas involuntarias en la implementación o configuración de los sistemas de seguridad | | Vulnerabilidades de seguridad | Posible | Moderado | RM |
| R24. Trasferencia no consentida de activos empresariales | | Pérdida de credibilidad y consecuencias legales | Posible | Alto | RA |

**Cuadro 14.** (Continuación)

| Identificación | | | Evaluación | | |
|---|---|---|---|---|---|
| Riesgo | Activo | Consecuencia | Probabilidad | Impacto esperado | Nivel de riesgo |
| R25. Modificación, eliminación o publicación de información sensible de la organización sin previa autorización. | PERSONAL | Pérdida de credibilidad y consecuencias legales | Posible | Alto | RA |
| R26. Soporte técnico deficiente para resolver problemas internos | | Retrasos en la operación | Probable | Moderado | RA |
| R27. Modificación mal intencionada de los parámetros de seguridad establecidos (Backus, firewall, antivirus, Etc.) | | Apertura de vulnerabilidades | Probable | Moderado | RA |

De la evaluación de riesgos y vulnerabilidades identificados en Move Cargo S.A. se lograron identificar los siguientes riesgos calificados como altos y que deben ser tratados dentro de la organización.

**Cuadro 15. Calificación de riesgos y vulnerabilidades**

| Calificación | Riesgos |
|---|---|
| Riesgo Catastrófico | R8, R9 y R17 |
| Riesgo Alto | R6, R10, R14, R15, R19, R20, R24, R25, R26 y R27 |
| Riesgo Medio | R1, R2, R3, R16, R18, R21 y R23 |
| Riesgo Bajo | R5, R7 y R22 |
| Riesgo Aceptable | R4, R11, R12 y R13 |

Para cada uno de los riesgos evaluados se tratará con política o procedimiento específico que ataque las causas de los riesgos y mitigue su impacto.

## 4.3 POLÍTICAS Y CONTROLES PARA CONTROLAR O MITIGAR RIESGOS Y VULNERABILIDADES DE LA ORGANIZACIÓN

Tomando en cuenta la declaración de aplicabilidad y el análisis de riesgos realizado se proponen políticas y controles acordes con la prestación del servicio, los riesgos y los requisitos y necesidades de las partes interesadas

### 4.3.1 Comprensión de la empresa y sus necesidades

Para poder determinar políticas efectivas con respecto a los riesgos y vulnerabilidades identificados se debe tener un entendimiento claro del contexto de la organización.

**Contexto de la organización:** Como medida para identificar los factores que pueden afectar los sistemas operativos de la organización se han identificado los siguientes factores internos y externos.

a) **Contexto Interno**

**Infraestructura tecnológica:** La organización conforme con las necesidades de los procesos, los requisitos de los clientes y la legislación vigente, ha establecido una infraestructura tecnológica la cual permita cumplir con el servicio ofrecido cumpliendo los requisitos identificados.

**Directrices:** La gerencia ha determinado los presupuestos y directrices que debe tener el departamento de infraestructura y tecnología para implementar el SGSI.

**Personal:** La organización cuenta con personal joven capacitado para el manejo de software operativo con facilidad y también se cuenta con personal con experiencia en manejo y prestación del servicio.

**Políticas de seguridad:** Se determinan políticas de seguridad de la información para ser implementadas en todos los niveles de la organización y se delegan responsabilidades para su implementación, control y mejora continua.

b) **Contexto Externo**

**Proveedores externos:** La empresa tiene contratado con proveedores la mayor parte del software operativo, contable y servicios necesarios para la operación (Internet, Correo, telefonía, datos. Etc.), estos proveedores son seleccionados, evaluados y reevaluados periódicamente según procedimientos y políticas para validar el cumplimiento de productos y servicios contra los requisitos de la organización y los clientes.

**Clientes:** Estos tiene requisitos específicos de comunicación ya que desean ser informados sobre sus procesos, los avances de cada uno y los trámites realizados.

**DIAN:** La organización debe sincronizar sus sistemas e infraestructura con los requisitos y necesidades del sistema de información utilizado por el estado para realizar las declaraciones de valor y poder prestar el servicio.

**Entorno económico:** La globalización y la apertura de mercados ha permitido expandir la economía hacia otros sectores y países lo que ha permitido tener un mayor número de competidores en busca de mantenerse en un mercado cada vez más competitivo.

**Requisitos legales:** La organización debe estar en la capacidad de cumplir con todos los requisitos legales establecidos por el gobierno para la prestación del servicio, incluidos los requisitos para el manejo del personal, pago de impuestos y prestación del servicio.

c) **Identificación de los sistemas operativos:**

Para la normal prestación del servicio de agenciamiento aduanero de la organización se lograron identificar los siguientes sistemas:

- ✓ Software operativo
- ✓ Sistema contable
- ✓ Correos electrónicos
- ✓ Acceso a internet

Para cada uno de los sistemas operativos se generan los siguientes protocoles y acciones.

d) **Software operativo:**

Funcionalidad: El software operativo es utilizado por la organización para prestar el servicio y tener una permanente comunicación con los sistemas operativos de la DIAN. Para la realización de declaraciones de valor.

Características: es una aplicación contratada con un proveedor externo el cual se encarga de mantener, actualizar y dar soporte. El software se encuentra instalado en los servidores de la organización y es administrado por el departamento de infraestructura y tecnología.

Caídas del sistema: En caso de una eventual falla del sistema operativo el departamento de infraestructura y tecnología con ayuda del proveedor empleara todas las herramientas que considere necesarias para restablecer el servicio de la manera más ágil posible. Como mecanismo de contingencia se cuenta con un software adicional en otro servidor con las mismas características, pero con una menor capacidad para ser utilizada por el departamento operativo.

e) **Sistemas contables**

Funcionalidad: El sistema contable administra la información financiera, los movimientos contables, las deudas con los acreedores, las cuentas por cobrar de los clientes y los valores de los impuestos.

Características: es una aplicación contratada con un proveedor externo especializados en el campo de manejo de información contable, este software es una aplicación web que puede administrase desde cualquier dispositivo, la información resultado de la actividad es almacenada en los servidores propios de la organización.

Caídas del sistema: En caso de una eventual falla del sistema contable el proveedor cuenta con soporte de 7*24 y un promedio de atención entre 1 y 3 horas. En caso que el fallo dure más del tiempo que el estipulado el proveedor envía a un técnico a las oficinas de la organización para que con colaboración de departamento de infraestructura busquen solucionen a los inconvenientes presentados.

f) **Correos electrónicos**

Funcionalidad: Permite tener una comunicación entre la organización, los clientes, los proveedores y todas aquellas partes interesadas en el sistema.

Características: El sistema de cuentas de correo electrónico es contratado con el proveedor de confianza de gran infraestructura que permite el envío y recepción de documentos de manera digital entre la empresa, los clientes, los proveedores y las demás partes interesadas de la organización.

Caídas del sistema: En caso de caídas del sistema por fallas leves, el proveedor de servicio garantiza la restauración del sistema en menos de 2 horas, en casos catalogados como falla media el proveedor garantiza la restauración del sistema en menos de 6 horas y en caso de fallas graves se garantiza la restauración del servicio en menos de 24 horas.

Estos son ejemplos de los tipos de fallas:

**Fallas leves:** Caídas del sistema o intermitencia de servicio.
**Fallas Medias:** Perdidas de la conectividad con los servidores o interrupción parcial del servicio.
**Fallas Graves:** Daños en la infraestructura como ruptura de fibra óptica, perdida de sistemas auxiliares o desconexión total de servidores.

g) **Acceso a internet**

Funcionalidad: Permite el acceso a las diferentes páginas web de la DIAN necesarias para la prestación del servicio, los tramites con terceros, la comunicación con las partes interesadas y la interacción con los diferentes actores del agenciamiento aduanero.

Características: Se contrata a un proveedor de confianza el cual sea reconocido en el mercado por prestar servicios de calidad. El servicio consta de un servicio de banda ancha que permita la transmisión de declaraciones de valor desde la organización hacia los sistemas informativos de la organización:

Caídas del sistema: El proveedor garantiza un correcto funcionamiento de servicio de internet con un tiempo estimado de funcionamiento sin intermitencia del 99%. Como medida de contingencia se cuenta con un segundo proveedor de Internet con un canal dedicado de punto a punto para la transmisión de declaraciones de valor.

### 4.3.2 Políticas de seguridad de la información

Teniendo en cuenta lo anterior se realiza la presente política de seguridad de la información, teniendo en cuenta las necesidades de la organización, el servicio que presta y el contexto en el que se desempeña.

Esta política se encuentra adecuada al tamaño de la organización, la cantidad de personal y la reglamentación aplicable teniendo encuentra el contexto identificado anteriormente

**Presentación de la Política de seguridad de SGSI**

Move Cargo S.A. consiente de la importancia que tiene la información para la prestación del servicio, la toma de decisiones y el cumplimiento de leyes vigentes a decidió tomar las acciones pertinentes y necesarias para proteger la información que genera, administra o trata minimizando o eliminado los riesgos.

Es responsabilidad del área de infraestructura y tecnología garantizar la seguridad por medio de la implementación de control establecidos en la presente política, para lo cual la administración suministra los recursos tecnológicos, humanos, financieros y logísticos necesarios para garantizar que la información se encuentre disponible, integra y confidencial en todo momento del ciclo.

Las acciones mencionadas en la siguiente política están basadas en la evaluación de riesgos y vulnerabilidades a las que se ve expuesta la organización por el servicio que ofrece, por el medio en el que se desempeña y la herramienta que utiliza para el tratamiento de la información.

La política de seguridad es puesta en conocimiento de toda la organización con el fin de crear cultura en la seguridad de la información.

**Objetivos de la política**

Como parte fundamental para el cumplimiento de los objetivos estratégicos y continuidad del negocio y apegados a los valores corporativos se establecen los siguientes objetivos:

- Minimizar o eliminar los riesgos que pudieran afectar la información de la organización.
- Ser base para la implementación de un sistema de gestión de seguridad de la información
- Fortalecer la cultura de seguridad de la información dentro de Move Cargo S.A.
- Garantizar que el hardware y software de la organización siempre se encuentre disponibles y estos no sea afectados por factores internos ni externos.

Teniendo en cuenta la evaluación de riesgo se implementa las siguientes políticas tendientes a eliminar las causas de los siguientes riesgos o vulnerabilidades.

### 4.3.2.1 Seguridad física y entorno

Riesgos relacionados con el entorno físico.

**Cuadro 16. Riesgos de seguridad – Entorno Físico**

| Riesgo | Evaluación |
|---|---|
| R8. Cuarto de sistemas sin medidas de seguridad | Riesgo Catastrófico |
| R9. Control de acceso físico a las oficinas inexistentes o deficientes | |
| R6. Hurto de hardware o activos de la infraestructura informática | Riesgo Alto |
| R1. Pérdida o daños en la infraestructura por eventos naturales. | Riesgo Medio |
| R2. Alteraciones del entorno de los sistemas de almacenamiento. | |
| R3. Acceso abusivo a los sistemas informáticos y operativos de la organización | |

**Parámetros de la seguridad física**

Como medida para garantizar la seguridad física de los equipos en los cuales se resguarda la información se toman las siguientes medidas:

- Se restringe el acceso a los servidores o cuartos de sistemas a todo el personal por medio de un sistema de seguridad perimetral resguardado bajo llave.
- Se dispone de los equipos de control de temperatura y humedad necesarios para garantizar el correcto funcionamiento de los equipos de almacenamiento.
- El acceso a los servidores se realiza bajo la autenticación de claves de seguridad.
- Se dispone de un sistema detección de fuego y sistemas de extinción de conflagraciones.

**Parámetros de la seguridad perimetral**

El responsable del sistema de seguridad utiliza las herramientas necesarias y coherentes suministradas por la organización para establecer el sistema de seguridad perimetral.

- ❖ Parametrizar un programa de antivirus de tal manera que evite el acceso y propagación de software maliciosos.
- ❖ Implementar un sistema de firewall que evita en acceso a páginas con contenidos peligrosos o indeseados.
- ❖ Implementar y controlar sistema de seguridad que permite la detección y control de intrusos externos.
- ❖ Parametrizar un sistema de seguridad de encriptación de acceso IP y acceso remotos lo que permite tener seguridad para los casos de accesos remotos.

### 4.3.2.2 Seguridad contra virus o malware.

Riesgos relacionados con la seguridad contra virus o cualquier tipo de software malicioso, ataques informáticos externos o daños lógicos en los software administrativos, operativos o contables.

**Cuadro 17. Riesgos de seguridad – Virus**

| Riesgo | Evaluación |
|---|---|
| R10. Propagación de virus o malware en los equipos de la organización. | Riesgo Alto |
| R14. Falta de control en las Instalaciones de software en los sistemas informáticos. | |

**Protección contra virus**

La organización implementa los controles necesarios y suficientes para minimizar los riesgos y vulnerabilidades del sistema al ser víctima de software malicioso.

- ❖ Se restringe el acceso a páginas web que tengan contenidos sexuales, redes sociales o que no se encuentre en redes seguras.
- ❖ Se restringe el acceso a páginas de música, videos o páginas con contenidos de entreteniendo y farándula.
- ❖ Se parametriza la necesidad de una segunda clave de administrador para realizar descargas de programas o ejecutables en todos los equipos de la organización.
- ❖ Se deshabilitan los puertos USB de todos los equipos para disminuir las vulnerabilidades de propagación de un virus por infección de una fuente externa (USB, discos duros, dispositivos móviles).
- ❖ Se Parametrizan los correos electrónicos para bloquear cualquier tipo de correo SPAM o usuarios de dudosa procedencia.
- ❖ Se prohíbe el acceso a internet para fines diferentes a los de la labor que desempeña.
- ❖ El administrador del sistema es el único habilitado para descargar e instalar programas desde sitios web.

### 4.3.2.3 Seguridad y control de usuario

Riesgos relacionados con los usuarios y la seguridad de los sistemas.

**Cuadro 18. Riesgos de seguridad – Usuarios**

| Riesgo | Evaluación |
|---|---|
| R24. Trasferencia no consentida de activos empresariales. | Riesgo Alto |
| R25. Modificación, eliminación o publicación de información sensible de la organización sin previa autorización. | |
| R26. Soporte técnico deficiente para resolver problemas internos. | |
| R23. Fallas involuntarias en la implementación o configuración de los sistemas de seguridad. | Riesgo Medio |

**Parámetros para el control de usuarios**

Se debe determinar una política de autenticación de usuarios la cual se debe encontrar aprobada por la organización y aplicada por todos los usuarios para lo cual se propone determinar los siguientes parámetros.

- Establecer un periodo de caducidad de la contraseña del usuario.
- Parametrizar usuarios y permisos para cada uno de los cargos de la organización teniendo en cuenta sus actividades y responsabilidades.
- Establecer reglas para la creación de contraseñas seguras. (utilizar en contraseñas mezclas de números, letras, minúsculas, mayúsculas y signos como: " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { | } ~.).

**Cultura organizacional**

Como medida para que la organización tenga una cultura basada en la protección de información, el responsable del SGSI debe fomentar la seguridad en todos los niveles de la organización con las siguientes actividades.

- Debe comunicar en todos los niveles relevantes del SGSI.
- Realizar charlas periódicas sobre sistemas de seguridad y prevención de ataques informáticos.
- Capacitar al personal nuevo sobre los sistemas de seguridad de organización y la importancia de los mismos.

### 4.3.2.4 Medios de información y BACKUPS

Riesgos relacionados con el respaldo de la información y los soportes del mismo.

**Cuadro 19. Riesgos de seguridad – Soporte de la información**

| Riesgo | Evaluación |
|---|---|
| R17. Fallas eléctricas o daños en la infraestructura eléctrica | Riesgo Catastrófico |
| R15. Daños en los soportes de la información | Riesgo Alto |
| R19. Intercepción de comunicación sensible o confidencial por medios magnéticos | |
| R20. Fallas en la planta telefónica, redes de internet o red WIFI | |
| R16. Perdida de los soportes de la información | Riesgo Medio |
| R18. Fallas en el suministro del servicio de comunicación (Internet, teléfono, correo) | |

**Copia de la información**

La organización implementa medidas para garantizar que en caso de materialización de alguno de los riesgos donde halla perdida, daño o modificación de la información esta se pueda recuperar de manera rápida y fiable.

- Se implementa sistemas informáticos que permita realizar copias de seguridad de la información de manera rápida y confiable.
- Implementar procedimientos de gestión de incidentes y recuperación de la información.
- Se cuenta con procedimiento de continuidad del negocio que permite retomar actividades en el momento que se materializa un riesgo calificado como alto o catastrófico.
- Se debe realizar actividades para garantizar que existan Backus de la información en memorias portátiles (Disco duros, servidores en la nube. etc.)

**Evitar las pérdidas de información**

Como parte integral de la política del SGSI se implementa las siguientes herramientas tendientes a la protección de la información para evitar pérdidas y por consecuencia retrasos, errores e inconformidades de cualquiera de las partes interesadas.

Para garantizar la disponibilidad el departamento de infraestructura de la organización implementa los siguientes protocolos de backup sobre la información que se considera sensible, importante o necesaria para la prestación del servicio.

Los sistemas utilizados por la organización para realizar los *backup* de los servidores donde se aloja la información de manera segura.

a) Backup diario: Este tipo de backup se realizará a la información necesaria para la prestación del servicio, así como la contable registrada. Este tipo de backup diarios se realizará de la siguiente manera.

b) Backup diario incremental: Para la información que es necesaria para la operación se determina realizar una copia de manera incremental para garantizar que un día de trabajo no se pierda. Se determinaron los siguientes horarios para realizar los Backups:

- ✓ 10:00 a.m.
- ✓ 12:00 a.m.
- ✓ 15:30 p.m.
- ✓ 18:00 p.m.
- ✓ 21:00 p.m.

Este tipo de backup solo almacena 1 copia de seguridad la cual sobrescribe modificando únicamente los archivos que han sido modificados o son nuevos.

c) Backup diario Completo: la información contable de la organización se le realizar backup de seguridad diariamente al finalizar el día para garantizar que los movimientos contables queden registrada y segura, para este caso solo se utiliza una copia completa en la tarde. El Backup se almacena de lunes a viernes a las 20:10 p.m.

d) Backup Nocturno: Considerada por la organización como información relevante para la prestación del servicio se realiza backup de los correos electrónicos del personal de confianza de la organización y el personal operativo, los cargos a los cuales se les realiza copia de seguridad son:

- ✓ Gerencia
- ✓ Dirección Operativa
- ✓ Dirección Administrativa y Financiera
- ✓ Dirección comercial
- ✓ Revisores
- ✓ Jefes de cuenta
- ✓ Jefes de Oficina puerto

El Backus se ejecuta los días jueves a las 20:10 pm

e) Backup Semanal: Para garantizar que la información considerada como indispensable, sensible o necesaria para la prestación del servicio se encuentre a salvo en caso de eventualidades que pudieran afectar la infraestructura física del SGSI de la organización, semanalmente el departamento de infraestructura y tecnología entrega a la dirección en un

disco extraíble un backup para que esta sea custodia por fuera de las instalaciones de la organización.

El backup semanal entregada a gerencia se realiza todos los días viernes o el día hábil anterior y se entrega la siguiente información.

Copia de la información operativa del primer backup incremental que se realiza el mismo día.

Ultima Backup de la información contable de la organización.

Ultimo Backup de los correos electrónicos del personal de confianza.

Estas medidas utilizadas por la organización para garantizar que no existirán perdidas de información considerables en el momento que se presentar un evento, riesgo o acto mal intencionado que afecte a los sistemas informáticos, la infraestructura física o la información de la organización.

#### 4.3.2.5 Riesgos aceptables

Los riesgos bajos y aceptables se controlan por medio de las políticas antes mencionadas y por los controles y revisiones realizadas tanto por la dirección, como por el departamento de talento humano.

**Cuadro 20. Riesgos de seguridad aceptables**

| Riesgo | Evaluación |
|---|---|
| R4. Fallas de equipos por cortes de energía o sobre carga en los equipos | Riesgos aceptables |
| R11. Software no licenciados | Riesgos aceptables |
| R12. Desarrollo propios con fallas de seguridad | |
| R13. Sistemas operativos obsoletos | |
| R5. Daños intencionales a la infraestructura de la organización | Riesgos bajos |
| R7. Manipulación de equipos sin controles | |
| R22. Personal con pocos conocimientos en informática o sistemas de seguridad | |

Como parte de la anterior política y como medida de control a continuación se describe la parte sancionatoria al personal que incumpla dichas políticas y reglamentos establecidos.

### 4.3.3 Sanciones o actos disciplinarios

Como medida para sancionar o tomar medidas disciplinarias contra los funcionarios o terceros que atenten contra la información, activos o estructura de la organización.

Clasificación de faltas:

a) Son faltas leves aquellas que el funcionario haya incumplido con los parámetros de seguridad establecidos en la política sin que estos afecten de manera significativa a la información, activos u estructura del SGSI.
b) Son faltas graves aquellas con las cuales al funcionario haya incumplido con los parámetros de seguridad establecidos y estos hayan afectado de manera moderada o significara la información, activos u estructura del SGSI.
c) Son consideradas faltas graves, toda vez que el funcionario cometa de manera reiterada o consiente se repitan tres veces.
d) Son faltas jurídicas todas aquellas que con intención, organización u negligencia del empleado afecten a la integridad, disponibilidad u confidencialidad de la organización y sus intereses.

La dirección determina las sanciones impuestas a los funcionarios por la realización de una falta grave de la siguiente manera.

a) Toda vez que por evidencia, designación o imputación de cargos sin que haya ninguna duda razonable un funcionario hayan cometido una falta.
b) leve por primera vez se les realizara un llamado de atención y debe asistir a una capacitación sobre seguridad informática.
c) Toda vez que por evidencia, designación o imputación de cargos sin que haya ninguna duda razonable un funcionario haya cometido una falta leve por segunda vez se le realizar un acto administrativo y se convocará a un comité disciplinario el cual podrá suspender del cargo hasta por dos días al funcionario no remunerables incluyendo el dominical.
d) Toda vez que por evidencia, designación o imputación de cargos sin que haya ninguna duda razonable un funcionario comete una falta leve por tercera vez, es considerado una falta grave y se tomaran las sanciones a las que haya lugar.
e) Toda vez que por evidencia, designación o imputación de cargos sin que haya ninguna duda razonable un funcionario comete una falta grave se realizara un acto administrativo y se convocara a comité disciplinario el cual dependiendo del acto puede tomar la decisión de suspender del cargo hasta

por un periodo de cinco días al funcionario o la desvinculación inmediata del funcionario.

f) En caso que exista una falta jurídica se tomaran las medidas disciplinarias, legales y administrativas a las que corresponda.

Todo acto considerado como una falta jurídica será administrado por el abogado de la organización con las entidades estatales correspondientes para imputar al funcionario los delitos cometidos con la organización.
Las sanciones establecidas son reglamentadas por la ley 1273 del 2009 capítulo I y II, las cuales serán solicitadas por la organización.

### 4.3.4 Mejora

Para que el sistema de gestión de seguridad de la información (SGSI) sea adecuado, eficaz y coherente con los objetivos y el servicio prestado por la organización este debe mejorar constantemente para lo cual se implementa las siguientes actividades.

- Auditoria al SGSI en periodos planificados por lo menos cada año.
- Informes periodos de la gerencia sobre la gestión del sistema.
- Revisión de las matrices de riesgos cada vez que existan cambios en los sistemas informáticos de la organización o cambios en los servicios prestados.
- Grado en el que se cumple los objetivos de la política de seguridad de la información.

# 5. CONCLUSIONES

Con los resultados obtenidos durante el proyecto se puede concluir que se logró cumplir con los objetivos propuestos ya que logro:

- Determinar en qué estado está la situación de la empresa en cuanto a la seguridad de la información.
- se diseñó un sistema de gestión del riesgo acorde al tamaño y necesidades de la organización en las que se incluye la identificación, evaluación y análisis de los riesgos en cuanto a la seguridad de la información.
- Y se propusieron políticas, controles y sistema de seguridad informática internos que permitirían a la Move Cargo S.A. controlar los riesgos y vulnerabilidades a los que se ven expuestos ya sea por la actividad que realizan o el medio en el que se ve obligados a trabajar.

Con la elaboración del proyecto se pudo determinar que aunque existen protocolos, procedimientos y responsables por la seguridad de la información estos no son suficientes para controlar los posibles impactos que generaría la materialización de uno de los riesgos considerados como altos.

Debido a la importancia de la información a la que tiene acceso Move Cargo por la actividad que desarrolla, es de vital importancia mantener un sistema que permita poder mantener segura, integra y confidencial y con la aplicación de los resultados obtenidos en el presente proyecto se puede realizar.

Con los pasos de mejora continua del Sistema de Gestión de la Seguridad de la Información, se garantiza que la organización independiente de los cambios en cuestiones internas y externas estos siempre estarán identificando, evaluado y controlando los nuevos riesgos y vulnerabilidades que se presentan en el ambiente tecnológico, actuando de manera preventiva evitando su materialización y por consecuente los posibles impactos.

# 6. RECOMENDACIONES

Del trabajo realizado se recomienda al Gerente de la Agencia de Aduanas Move Cargo S.A implementar en un periodo no mayor a 6 meses el Sistema de Gestión de la Información con los controles definidos en el proyecto.

También se recomienda que el departamento de Infraestructura y Tecnología vigile la efectividad de los controles implementados, así como la divulgación a todo el personal de las políticas de seguridad y las medidas disciplinarias que tomaran en el caso que alguno empleado atente contra la seguridad de la información.

Para mantener el Sistema de Gestión de la información seguro, conforme y adecuado con la organización y el negocio, se recomienda realizar revisiones periódicas a los objetivos del sistema, así como actualización de los controles implementados según se detecte la necesidad o se evidencie que el riesgo aumente.

La gerencia y la dirección debe estar atentos a las nuevas tecnologías, herramientas y dispositivos que se utilicen para la prestación del servicio ya que incorporar nueva tecnología sin un análisis de vulnerabilidades puede generar un riesgo para la organización y la finalidad de este trabajo.

## BIBLIOGRAFÍA


AGUIRRE CARDONA Juan David, ARIZTIZABAL BETANCOURT Catalina. Diseño de un sistema de gestión de seguridad de la información para el grupo empresarial la OFRENDA, Proyecto de grado, Pereira universidad tecnológica de Pereira, Facultad de Ingeniería, programa de ingeniería de sistemas de computación, 2013, 82 p.

Blog Especializados en sistemas de gestión de seguridad de la información, ¿Qué es el CIA? Confidencialidad, integridad y disponibilidad [En línea] <https://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion> [citado 2018].

Blog Especializados en sistemas de gestión de seguridad de la información, ISO 27001: Ciclo Deming [En línea] <https://www.pmg-ssi.com/2015/06/iso-27001-ciclo-de-deming/> [citado 2018].

Blog Especializados en sistemas de gestión de seguridad de la información, ISO 27001: Como implementar políticas de gestión de un sistema de Gestión de Seguridad de la Información. [En línea] <https://www.pmg-ssi.com/2014/03/iso-27001-como-implantar-politicas-de-gestion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/ > [citado 2018].

Colombia. MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO. Decreto 390 (7 de marzo 2016). Por el cual se establece la regulación aduanera. Bogotá D.C. el ministerio 2016. 311 p.

Colombia. MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO. Decreto 390 (7 de marzo 2016). Sección 1. Artículo 54. Agencia de aduanas. Bogotá D.C. el ministerio 2016. 41 p.

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRONICA. Metodología de análisis y gestión de riesgos de los sistemas de información: Ministerio de hacienda y administración pública, libro I – método, 2012, 127 p, NIPO: 630-12-171-8

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRONICA. Metodología de análisis y gestión de riesgos de los sistemas de información: Ministerio de hacienda y administración pública, libro II – Catalogo de elementos, 2012, 75 p, NIPO: 630-12-171-8

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, PROCEDIMIENTOS E IMPULSO DE LA ADMINISTRACIÓN ELECTRONICA. Metodología de análisis y gestión de riesgos de los sistemas de información: Ministerio de hacienda y administración pública, libro III – Guía de técnicas, 2012, 42 p, NIPO: 630-12-171-8

Gestión del riesgo en la seguridad informática, Análisis de riesgo [En línea] <https://protejete.wordpress.com/gdr_principal/analisis_riesgo/> [citado 2018].

GIRALDO CEPEDA Luis Enrique. Análisis para la implementación de un sistema de gestión de la seguridad de la información según norma ISO 27001 en la empresa SERVIDOC S.A. proyecto de grado, Cali Universidad Abierta y a distancia UNAD, Especialidad en seguridad informática, 2016, 206 p.

Gobierno TI, Arquitectura TI Colombia, [En línea] < http://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8078.html> [citado 2017].

GUSTAVO Pallas Mega, Metodología de Implantación de un SGSI en un grupo empresarial jerárquico, Tesis maestría, Montevideo Uruguay, Universidad de Republica, Facultad de ingeniería, 2009, 195 p.

GUZMÁN GARCÍA Alexandra; TABORA BEDOYA Carlos Alberto, Diseño de un sistema de gestión de la seguridad de la información SGSI para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C. a través de la auditoria, Trabajo de grado, Bogotá, Universidad Nacional Abierta y a distancia – UNAD, Especialidad en seguridad informática, 2015, 311 p.

GUZMAN SILVA Carlos Alberto, Diseño del sistema de gestión de seguridad de la información para una entidad financiera de segundo piso, Trabajo de grado, Bogotá, Universidad politécnico Gran Colombiano, Especialidad en seguridad informática, 2015, 173 p.

INSTITUTO COLMBIANO DE NORMAS TECNICAS Y CERTIFICACIÓN. Tecnología de la información: Vocabulario: ICONTEC. 2013: (NTC-ISO 27000)

INSTITUTO COLMBIANO DE NORMAS TECNICAS Y CERTIFICACIÓN. Tecnología de la información: Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos: ICONTEC. 2013: (NTC-ISO 27001)

INSTITUTO COLMBIANO DE NORMAS TECNICAS Y CERTIFICACIÓN. Tecnología de la información: Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos: ICONTEC. 2013: (NTC-ISO 27001)

Mendoza Miguel Angel, Welivesecurity, ¿Cómo definir el alcance del SGSI [En línea] <https://www.welivesecurity.com/la-es/2018/01/09/definir-alcance-sgsi/> [citado 2018].

SANCHEZ ARIAS julia Inés. Nueva regulación aduanera en Colombia, aspectos didácticos de la parte sustantiva. Bogotá D.C, 2017, 170 p.

VILLENA AGUILAR Moisés Antonio. Sistema de gestión de seguridad de información para una institución financiera, Tesis de grado, Lima Perú, Pontificia Universidad católica del Perú, Facultad de ciencias e ingeniería. 2006, 72 p.

# 5 ANEXOS

## 5.2 RESUMEN ANALÍTICO ESPECIALIZADO (RAE)

**Cuadro 21.** RAE

| | |
|---|---|
| **Título** | DISEÑO DE UN SISTEMA DE GESTIÓN EN SEGURIDAD INFORMÁTICA (SGSI) EN LA AGENCIA DE ADUANAS MOVE CARGO S.A. NIVEL 1. |
| **Autor** | Ing. Ana María Bohórquez Muñoz |
| **Fecha** | Septiembre 24 de 2017 |
| **Palabras claves** | Seguridad de la información, disponibilidad, integridad, confidencialidad, eficaz, coherente. |
| **Descripción** | Este proyecto diseña un sistema de gestión de seguridad informática bajo la norma ISO 27001 para la Agencia de Aduanas Move Cargo S.A Nivel 1. Teniendo en cuenta el contexto interno y externo de la organización, el servicio prestado, la reglamentación aplicable y la declaración de aplicabilidad. |
| **Fuentes** | Para la realización de este proyecto se tomó como base los siguientes textos:<br>➢ NTC – ISO 27000<br>➢ NTC – ISO 27001<br>➢ NTC – ISO 27005,<br>➢ Libros I, II, III, Metodología Magerit |

**Fuente:** Propia

**Cuadro 8.** (Continuación)

| | |
|---|---|
| **Contenido** | El proyecto contiene la siguiente información relevante para cumplir con los objetivos planificados:<br>➢ Objetivos planificados<br>➢ Información recolectada<br>➢ Resultados obtenidos<br>➢ Propuestas realizadas<br>➢ Análisis realizados<br>➢ Conclusiones del proyecto |
| **Metodología** | La metodología usada para este proyecto es Cuantitativa ya que se realiza un análisis del estado actual de la organización en cuanto a la seguridad del sistema de información en la Agencia de Aduanas Move Cargo S.A. Nivel 1. |
| **Tipo de investigación** | El tipo de investigación para este proyecto es correlacionar ya que se validar la relación que existe entre los paramentos del sistema de seguridad informática y los ataques informáticos. |
| **Conclusiones** | Se puede concluir que con el diseño de un sistema de gestión de seguridad informático dentro de los procedimientos de la Agencia de Aduana Move Cargo S.A. Nivel 1. Estará preparada para asumir, disminuir, eliminar o trasferir los riesgos y amenazas que se puedan presentar en la organización que pudiera afectar la información. |
| **Recomendaciones** | Es importante poder mantener el SGSI diseñado acorde con las características de la empresa, el medio el que se desempeña, el servicio prestado y la reglamentación aplicable por lo cual se recomienda que se establezca capacitaciones sobre nuevas tecnológicas y metodologías de seguridad constantemente a los involucrados y a la gerencia |